

Fermi National Accelerator Laboratory

**Title**

Policy on Controlled Unclassified Information (CUI)

**Policy Number**

KB0013638 v4.0

**Details**

**Policy on Controlled Unclassified Information (CUI)**

**1. Purpose**

This policy establishes the requirements and standard approach for compliance with DOE Order 471.7, Controlled Unclassified Information.

This Policy is not a contract and is not intended to create any obligations on Fermi Research Alliance (FRA). This Policy may be terminated or changed by FRA at any time, with or without notice.

**2. Scope**

The scope of this policy covers the entirety of FRA s activities that are considered CUI-generating, and information held by FRA that is CUI.

**3. Applicability**

This Policy applies to Fermi Research Alliance, LLC and all its employees, affiliates, and users.

**4. Effective Date and Date Reviewed/Updated**

This Policy went into effect on July 31, 2023. This policy replaces the Policy on Official Use Only Documents.

## 5. Policy

CUI-1: Fermilab will mark CUI in accordance with the CUI Registry and will only use categories found in the CUI Registry for identification, marking, safeguarding, and disseminating.

CUI-2: Except for Unclassified Controlled Nuclear Information (UCNI) and Naval Nuclear Propulsion Information (NNPI), CUI markings are the only markings Fermilab will use to designate documents and matter containing CUI. Non-Federal CUI may be exempt from marking.

CUI-3: Fermilab will keep track of all CUI-marked information submitted to the Office of Scientific and Technical Information (OSTI). Fermilab will also notify OSTI when CUI-marked information previously provided to OSTI has its marking changed.

CUI-4: Fermilab will follow the latest version of NIST 800-53 to implement applicable controls for Federal/Contractor CUI-holdings to the moderate level.

CUI-5: Fermilab will ensure all non-Federal third-party CUI-holding systems are compliant with NIST 800-171, unless the system has specific requirements needing a higher level of protection.

CUI-6: Fermilab personnel will ensure that when CUI is found outside of normally implemented physical & environmental security controls, personnel will ensure that they have direct control of CUI material, or it is reasonably protected behind at least one physical barrier and cannot be accessed.

CUI-7: If a document is suspected of containing CUI, but is not marked as such, then Fermilab will protect the document as if it is CUI until it can be reviewed.

CUI-8: If CUI has been reproduced or shared, Fermilab will protect the reproduced CUI with the same controls as the original CUI document.

CUI-9: Fermilab will ensure that when CUI is reproduced by physical means, the machine used will not retain the CUI-specific data. Other data, i.e. metadata, may be retained.

CUI-10: Fermilab will ensure all employees, users, and temporary staff who interact with CUI will receive CUI-specific training.

CUI-11: Fermilab will only grant access to CUI on a need-to-know basis.

CUI-12: Fermilab, when sending CUI via email outside of Federal IT systems, will ensure that the CUI is an attachment, encrypted, protected by a password. The password to the CUI document must be transmitted separately from the email containing CUI.

CUI-13: Fermilab will treat legacy Official Use Only (OUO) material as if it contains CUI and will safeguard it in accordance with other standard CUI controls.

CUI-14: For legacy OOU documents that cannot be safeguarded as CUI, Fermilab will develop alternate plans for document protection, and this plan will be reviewed by the Departmental Element Designated CUI Official or designee for approval.

CUI-15: Fermilab will remove the CUI markings on documents that are determined to no longer warrant protection as CUI.

CUI-16: Fermilab will decontrol CUI that is being sent to National Archives and Records Administration (NARA). When CUI cannot be decontrolled, it must be indicated on a Transfer Request (TR) in NARA's Electronic Records Archives (ERA), or on an SF 258 paper transfer form, that the records should continue to be controlled as CUI.

CUI-17: Fermilab, when destroying CUI of a physical, digital, and optical nature, will ensure that it is unreadable, indecipherable, and irrecoverable.

CUI-18: Fermilab will procure the services of a commercial National Association for Information Destruction (NAID)-certified document destruction company. The Fermilab CUI Team will ensure locked bins are placed in locations throughout Fermilab grounds and are within quick reach of all Fermilab employees. CUI no longer needed will be deposited in locked bins. On a regular schedule, the NAID-certified document destruction company will receive these bins, and all contents will be destroyed to the extent that they are unreadable, indecipherable, and irrecoverable.

CUI-19: If the misuse of CUI may result in the document being released to unauthorized persons, Fermilab will report the misuse to the Departmental Element and Site Office Designated CUI Officials as soon as possible. Reporting will also include notifying the DOE Office of the Inspector General (OIG) if necessary, per OIG requirements.

CUI-20: Fermilab will conduct annual maturity assessments of CUI controls as part of a self-inspection program to track their implementation across directorates and prepare a maturity report on the implementation of CUI controls at least annually.

CUI-21: Fermilab will maintain a formal Request For Comments (RFC) program that will allow for Fermilab team members to submit comments on the CUI Standard & Guidelines (e.g., comments about changing controls, changing the wording of controls, etc.)

CUI-22: Fermilab will ensure that for all third-party solutions that are procured on contract (e.g., Software as a Service solutions) stipulate that all CUI data is destroyed per CUI-17 requirements at the end of the business relationship, and the third party no longer holds onto any CUI data.

## **6. Definitions**

Fermilab is the physical site and property that is the Fermi National Accelerator Laboratory.

Fermi Research Alliance, LLC is the operator and manager of the Fermi National Accelerator Laboratory under Department of Energy Prime Contract No. DE-AC02-07CH11359 and is the principal employer of personnel working at Fermilab.

CUI, or Controlled Unclassified Information, is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended. For Fermilab, CUI is information that has a federal aspect to it, by way of federal funding and federal interest, and is *not* intended for open publication. CUI does not include information contained in contractor-owned records as defined by FRA s prime contract with the DOE.

The Departmental Element Designated CUI Official is the designated official who oversees the implementation of the requirements in DOE Order 471.7 within their element (with the elements being the DOE Offices, such as Office of Science, Office of Electricity, office of Environmental Management, etc.)

## 7. Responsibilities

The Fermilab CISO is accountable for DOE Order 471.7 being implemented across Fermilab.

The Fermilab CUI Team Lead, reporting to the CISO, is responsible for DOE Order 471.7 being implemented across Fermilab.

## 8. Authorities

[DOE Order 471.7, Controlled Unclassified Information.](#)

## 9. Owner

The Fermilab CISO is the owner of the policy.

## 10. Review Cycle

This Policy shall be reviewed every year.

## 11. Communication Plan

The requirements of this Policy shall be communicated by the CUI Team Lead to all employees, affiliates, and users and periodic training shall be provided to Requirement Owners and ALD/Senior/Office/Project Directors. This Policy shall be available on the Fermilab policy website. The CISO is responsible for the successful communication of this Policy.

---

Updated	2023-08-01 18:09:43 by annacamp
Published	2023-08-01
Valid	2024-08-01

---