

**University of California  
Policy on Accountable Classified Removable Electronic Media**

**Contents**

<b>I. PREAMBLE .....</b>	<b>1</b>
<b>II. DEFINITIONS, ACRONYMS, AND INITIALISMS .....</b>	<b>2</b>
<b>III. STATEMENT OF REQUIREMENTS .....</b>	<b>3</b>
A. Variances.....	3
B. Training.....	3
C. Accountable CREM.....	3
D. Accountability System.....	4
E. Creation of Accountable CREM.....	5
F. Marking.....	5
G. Ownership.....	5
H. Transfers .....	6
I. Storage .....	7
J. Destruction.....	7
K. Inventories.....	8
L. Missing Accountable CREM .....	9

# **University of California**

## **Policy on Accountable Classified Removable Electronic Media**

*Effective: March 3, 2004*

### **I. PREAMBLE**

The President of the University of California intends that there be a consistent and uniform approach for managing accountable classified removable electronic media (CREM) at all of the national laboratories it manages. This document

- establishes common practices to comply with specific DOE/NNSA requirements for accountable CREM and
- adopts the best practices that have been identified by the Lawrence Livermore National Laboratory (LLNL) and the Los Alamos National Laboratory (LANL).

The University of California Laboratories will manage their accountable CREM with the following vision:

- LLNL and LANL shall establish full personal responsibility for accountable CREM.
- Each site shall use a single site wide accountability system except for accountable CREM that is COMSEC, Sensitive Compartmentalized Information (SCI), or in a Special Access Program (SAP); these categories will be accounted for using programmatic guidance.
- Using a graded approach, each site shall implement applicable requirements specified in DOE Manual 471.2-1C, "Classified Matter Protection and Control Manual," and supplemented by DOE Order 471.2A, "Information Security Program," or their successors. Such implementation will ensure that the level of effort and resources expended to control and manage accountable CREM are commensurate with the level of risk associated with that matter.
- Accountable CREM will be managed from creation to destruction.
- LANL and LLNL will communicate with and ensure that those handling or otherwise utilizing classified media are aware of and implement this policy.
- The quantity of accountable CREM will be minimized using available procedures and technologies, such as media-less systems in the user environment.

The University of California also expects that LANL and LLNL will take appropriate actions when the requirements for accountable CREM have been violated. These actions include the sharing of security incident information that broadly describes what happened, what causal factors were involved, and how future, similar events can be prevented.

The Director, Safeguards and Security, Laboratory Management Office, University of California Office of the President, will provide change control and issue future revisions to this policy document.

## II. DEFINITIONS, ACRONYMS, AND INITIALISMS

CMPC	Classified Matter Protection and Control
CREM	Classified electronic media are those materials and components manufactured to provide nonvolatile storage of classified digital data that can be read by a computer. “Removable” refers to such media that are <ul style="list-style-type: none"><li>• designed to be introduced to and removed from the computer without adverse impact on computer functions, <i>or</i></li><li>• separated from the computer for any reason, <i>or</i></li><li>• portable electronic devices.</li></ul>
Custodian/CAS <sup>1</sup>	An approved, trained, and knowledgeable person who is responsible for maintaining all records and administrative controls for classified matter received by and or dispatched from the accountability system.
DOE	Department of Energy
LADS	Laboratory Administrative Document System
legacy CREM	CREM created before the DOE requirement specific to CREM accountability management was issued.
mass move	Physical relocation of the entire inventory of CREM managed by a Custodian/CAS.
mass storage systems	Centralized systems that back up and archive electronic data and that by virtue of their design and operation preclude the removal of media without detection.
media library	A location in which a collection of CREM is kept under the control of a designated Custodian/CAS.
NNSA	National Nuclear Security Administration
owner	The person to whom the accountable CREM is assigned in the accountability system.
transfer	A change of ownership.

---

<sup>1</sup>The term “Custodian/CAS” in this document covers the functions that are performed by a “Custodian” at LANL and a “Classified Administrative Specialist” (CAS) at LLNL. This distinction is necessary because at LLNL the “Custodian” corresponds to a “User” at LANL. Site-specific terminology is allowed so long as all of the responsibilities are fulfilled by the same position.

### **III. STATEMENT OF REQUIREMENTS**

#### **A. Variances**

1. DOE Variances  
Any proposed practices for CREM that deviate from the requirements of DOE O 471.2A or DOE M 471.2-1C must be addressed in a security plan that proposes alternate or equivalent practices that will be implemented in lieu of the DOE/NNSA requirement. After approval by the requesting Laboratory, this security plan will be submitted to DOE/NNSA.
2. UC Variances  
Any proposed practices that deviate from practices specified by this policy will be addressed in a security plan that specifies the actions that will be implemented in lieu of the UC practice. After approval by the requesting Laboratory, the security plan must be approved by the University of California's Director of Safeguards and Security.
3. Local Security Plans  
The CMPC Manager for each site must approve security plans required by this policy before the practice covered by the plan is implemented.

#### **B. Training**

1. Each Laboratory must document and centrally manage training on the handling of accountable CREM and the authorization process for Custodian/CAS.
2. Before being authorized to perform the functions assigned to a Custodian/CAS, the Custodian/CAS must receive documented training in both accountable CREM handling and in being a Custodian/CAS.
3. No one is authorized to be an owner of accountable CREM without prior training in handling accountable matter.
4. Line managers responsible for Custodian/CAS and owners must receive documented training.

#### **C. Accountable CREM**

1. Unless otherwise stated in this document or covered by a DOE or UC variance, CREM containing the following data will be entered into accountability:

- Top Secret (TS);
  - Secret Restricted Data (SRD);
  - Sigma 14 and 15;
  - Secret CREM stored outside a Limited Area (or higher);
  - Deployable Nuclear Emergency Search Team (NEST) and Accident Response Group (ARG) operations;
  - Cryptography and designated COMSEC<sup>2</sup>;
  - NATO ATOMAL;
  - Designated United Kingdom information;
  - Special access programs (for example, designated SAPs)<sup>2</sup>.
2. Classified laptop computers with fixed internal hard-drives storing data listed in III.C.1.
  3. Electronic storage media are excluded from accountability as long as they are
    - protected by multiple layers of physical security *and*
    - a computer system design that precludes undetected removal of the media.
  4. Organizations that utilize electronic disk farms, multimedia backup units, or similar electronic mass storage devices with system software and/or system device registries capable of verifying the presence of their classified media must use this capability as a tracking system for these media if they are excluded from accountability under III.C.3.
  5. CREM exempted from inclusion in an accountability system in III.C.3 must be entered into an accountability system once separated from the parent computer or mass storage system.
  6. Newly created media that are immediately destroyed following their use for file transfers need not be entered into accountability if the specific destruction process is documented in an approved security plan.
  7. There is no requirement to enter into a LANL or LLNL accountability system CREM that is owned by another laboratory or agency and is brought to LANL or LLNL for temporary use and/or storage by an employee of another laboratory or agency.

#### **D. Accountability System**

1. Procedures must be developed, documented, and communicated to ensure that all accountable CREM not exempt from formal accountability (Section III.C.3; COMSEC, SCI, and SAP material) is entered into the accountability system.

---

<sup>2</sup>CREM in these categories will be accounted for using programmatic guidance or other rules established by the program or agency responsible for this information. CREM in these categories are exempt from the requirements of this policy if managed in a separate accountability system.

2. Any unique label, such as a vendor-provided serial number, associated with a piece of media can be used to meet the requirement that each piece of accountable CREM be uniquely identified. An additional barcode or other site-specific identification marker need not be used so long as the unique identifier used is recorded in the accountability system record.
3. If barcodes are used to track media in the Laboratory-wide single accountability system, each Laboratory must ensure that no duplicate numbers are issued.

#### **E. Creation of Accountable CREM**

1. Creators of accountable CREM must ensure that accountable CREM is marked and entered into the accountability system
  - the day it was created *or*
  - if it was created after normal hours, by close of business the following business day.
2. The creator of CREM is the CREM owner, and must follow the requirements in Section III.G, until a transfer is made.

#### **F. Marking**

1. CREM must be marked with the accreditation level of the information system unless
  - an appropriate classification review has been conducted or the information has been generated by a tested program verified to produce consistent results and approved by the Designated Accrediting Authority (DAA), *or*
  - the required marking is impractical or interferes with operation of the media. Alternate marking procedures must be documented in an approved security plan.
2. Media markings must follow DOE policy.

#### **G. Ownership**

1. Ownership of accountable CREM will be assigned to a person, *not* a location. A UC variance will be considered for special circumstances such as media libraries.

2. A person must accept the associated responsibilities for accountable CREM by signing a receipt when he or she is assigned ownership of the accountable CREM.
3. Owners are responsible for the accuracy of the information contained in the accountability system for their CREM.
4. Custodians/CAS must provide the owners with the information contained in the accountability system for review.
5. The Custodian/CAS will update the accountability system with any corrections identified by the CREM owner.

## H. Transfers

1. Change of Ownership (Transfer)
  - a. All transfers of accountable CREM must be processed through the sending and receiving Custodian/CAS.
  - b. All transfers of ownership of accountable CREM must be made by a receipt.
  - c. The Custodian/CAS maintains a copy of the receipt for transfer of accountable CREM.
  - d. A signed copy of the receipt must be returned to the sending Custodian/CAS
    - within 4 working days of receiving the accountable CREM if the transfer is on site, *or*
    - within 30 working days of receiving the accountable CREM if the transfer is from another site.
  - e. The creator of CREM must ensure the CREM is entered into accountability by a Custodian/CAS (Section III.E.1) and any transfer of CREM by the creator to another owner must be processed in a manner identical to any change of ownership.
2. The Custodian/CAS will open classified mail and, if the mail contains accountable CREM, update the accountability records to reflect the new owner and/or location. *Note:* Only the addressee may open classified mail marked “to be opened by addressee only.”
3. On the day of the change or by close of business the following business day if it the change occurs after normal hours, the Custodian/CAS must record the following:
  - CREM location change, even if there is no transfer of ownership, *and*

- CREM organization change, even if ownership of the CREM does not change.
4. For mass moves an approved security plan is required and must specify
    - how CREM will be accounted for before, during, and after the move, *and*
    - the timeframe within which these functions must be accomplished.

## **I. Storage**

1. GSA-approved security containers used to store accountable CREM must
  - be entered into a property management or other tracking system, *and*
  - not be moved without updating the tracking system.
2. The CREM accountability records must be updated (Section III.H.3) to reflect the new location of the security container.
3. Accountable CREM shall not be stored in the Laboratory's Records Center with the following exception: only the organization that owns the Records Center may store its own accountable CREM in the Records Center.
4. Classified matter that has been maintained in the Laboratory's Records Center prior to the effective date of this policy, for which access is restricted to Q-cleared personnel, does not need to be retrieved and reviewed for the presence of accountable CREM while in these storage locations. However, if removed from these storage locations, the classified matter must be promptly examined for the presence of CREM.
5. Any legacy CREM that is determined to be accountable must be immediately entered into accountability, even if the decision is made to destroy it promptly.
6. Accountable CREM may be transferred to the Laboratory's Archives Facility if the ownership of the CREM is transferred to a person in that facility who will assume the ownership responsibilities for that accountable CREM.

## **J. Destruction**

1. Accountable CREM must be destroyed according to specifications in DOE M 471.2-1C.
2. An appropriately cleared person other than the person destroying accountable CREM must witness its destruction.
3. The Certificate of Destruction must include the signature and names of the persons who destroyed the accountable CREM, their organization, and the date. Records of destruction must be retained as specified by DOE M 471.2-1C.

4. Both the destroyer and the observer must sign the certificate of destruction and return the signed certificate to the Custodian/CAS.
5. The Custodian/CAS shall provide a copy of the certificate of destruction of the accountable CREM to the owner.
6. The destruction of accountable CREM and the date must be recorded in the accountability system.
7. Accountable CREM must not be recorded as “destroyed” in the accountability system until the Custodian/CAS receives the certificate of destruction.
8. If the CREM is destroyed within one week of being delivered to the Custodian/CAS for destruction, the Custodian/CAS does not have to be listed as the owner of the accountable CREM.
9. See Section III.C.6 regarding CREM created for and destroyed immediately following file transfers.

## **K. Inventories**

1. NEST/ARG deployable CREM must be inventoried once a month by two appropriately cleared persons.
2. All other accountable CREM must be inventoried annually between August and October.
3. The Custodian/CAS and one other cleared person must visually verify all accountable CREM at the time of the inventory. **Note:** The Custodian/CAS may conduct the inventories alone if a barcode reader is used.
4. A full inventory of accountable CREM must be done in accordance with the security plan for any mass move.
5. When a Custodian/CAS changes, the incoming Custodian/CAS may demand a full inventory of the accountable CREM for which they are assuming responsibility as the Custodian/CAS.
6. In addition to the annual inventory, each Laboratory may at any time call for a full or partial inventory of its accountable CREM.
7. Personnel overseeing CMPC requirements must be provided access to any area in which accountable CREM is stored.
8. Owners must make their accountable CREM available to the inventory officials.
9. Accountable CREM that cannot be presented for inventory by the owner/owner’s organization is considered missing (Section III.L).

## **L. Missing Accountable CREM**

1. Whenever CREM cannot be presented or located by the owner/owner's organization, it is considered missing and must be reported immediately to the Laboratory's security inquiry organization.
2. The Laboratory must use the next 24 hours to conduct a more thorough search for the missing accountable CREM.
3. In accordance with requirements for reporting incidents of security concern, if the missing accountable CREM cannot be found within the 24-hour search period, a report must be submitted to the DOE site office having oversight of the Laboratory. A report must also be made to the DOE Emergency Operations Center (EOC) in accordance with DOE N 471.3, Reporting Incidents of Security Concern. Reporting to both the site office and the DOE EOC is the responsibility of the Laboratory's security organization.