

UC Davis Policy and Procedure Manual

Chapter 310, Communications and Technology

Section 75, Whole Disk Encryption

Date: 5/29/07

Supersedes: New

Responsible Department: Information and Educational Technology

Source Document: Business and Finance Bulletin IS-3, Information Security

I. Purpose

This section establishes use of whole disk encryption for the storage of restricted electronic information consistent with campus need for continued availability of the information. This section applies to the storage of academic and administrative restricted electronic information and its users.

II. Definitions

Additional terms used in this section are defined in Sections 310-23 and 310-24.

- A. Cryptography—method used to encode information so only authorized individuals can access the information.
- B. Electronic storage media—electronic systems used to record, index, store, preserve, or retrieve data files, including portable storage systems.
- C. Encryption—transforming information using a secret key so that the information is unintelligible to unauthorized parties.
- D. Key escrow—mechanism that permits an authorized third party to decrypt files.
- E. Restricted electronic information—electronic information for which content requires protection from unauthorized create, read, modify, or delete functions; including but not limited to personally identifiable information protected by federal or state law.
- F. Whole disk encryption—encryption to an electronic storage system that may exclude a system or boot partition.

III. Policy

- A. Whole disk encryption shall be used to secure restricted electronic information stored on laptop computers and electronic storage media for which physical security controls are limited due to the mobile nature of the computer or storage media, and for desktop computer systems located in areas with public access or with no physical theft deterrents.
- B. Authorized access to encrypted University information shall be preserved. Access by individuals other than the data custodian shall be administered under the provisions of Section 310-24.
- C. Deployment of a whole disk encryption service by a campus unit shall use the campus infrastructure cryptography service. Exceptions must be approved by the Information Security Coordinator (see V, below).

IV. Responsibilities

- A. Users and system administrators
 - 1. Identify restricted electronic information subject to encryption.
 - 2. Safeguard encryption security pass phrases, encryption keys, or authentication devices.
 - 3. Use encryption consistent with University policy.
 - 4. Remove unneeded restricted information from electronic storage media whenever possible.

- B. Department head
 - 1. Approve use of encryption on restricted information within the department.
 - 2. Ensure cryptography use is consistent with campus and University policy.
 - 3. Authorize use of key escrow service to access encrypted devices, consistent with University privacy policies.
 - 4. Consult with the Information Security Coordinator as needed to select a reasonable and practical data security solution.
- C. Information Security Coordinator
 - 1. Publish cryptography infrastructure standards for whole disk encryption.
 - 2. Maintain and publish list of cryptography products compatible with encryption infrastructure.
 - 3. Approve requests for exceptions to the standard campus infrastructure cryptography service.
 - 4. Approve use of key escrow/recovery services to access encrypted devices.
- D. Information and Educational Technology
 - 1. Administer and maintain hardware and software supporting cryptography infrastructure.
 - 2. Publish resources for use of cryptography infrastructure.

V. Exceptions

Requests for exception from the use of a campus whole disk encryption product shall be submitted to the Information Security Coordinator and must contain the following information.

- A. Unit requesting exception.
- B. Contact information for unit director/manager.
- C. Contact information for unit technical representative.
- D. Date of request.
- E. Proposed alternate solution.
- F. Reason why proposed alternate solution is being requested.
- G. Logical and physical security controls or practices that ensure any unauthorized activity threatening the confidentiality, integrity, or availability of the encryption system or server stored encryption key(s)
 - 1. will be logged;
 - 2. are subject to timely review; and
 - 3. will be reported to the Information Security Coordinator (when appropriate).
- H. Acknowledgement that the use of key escrow function requires appropriate approval as described in Section 310-24.

VI. Further Information

Additional information is available from the Information Security Coordinator, Information and Educational Technology (<http://security.ucdavis.edu>).

VII. References and Related Policies

- A. UC Office of the President Business and Finance Bulletins:

1. IS-3, Information Security.
 2. RMP-8, Legal Requirements on Privacy of and Access to Information.
- B. UCD Policy and Procedure Manual:
1. Section 310-22, Cyber-Safety Program.
 2. Section 310-23, Electronic Communications—Allowable Use.
 3. Section 310-24, Electronic Communications—Privacy and Access.
 4. Section 320-20, Privacy of and Access to Information.
 5. Section 320-21, Disclosure of Information from Student Records.
 6. Section 320-22, Collection and Confidentiality of Social Security Numbers.
 7. Section 320-35, Privacy of Health Information.
 8. Section 320-36, Access to Protected Health Information for Research.