

UC Davis Policy and Procedure Manual

Chapter 310, Communications and Technology

Section 22, UC Davis Cyber-Safety Program

Date: 5/14/09

Supersedes: 4/25/05

Responsible Department: Information and Educational Technology

Source Document: Business and Finance Bulletin IS-3

Exhibit A, UC Davis Security Standards

I. Purpose

This policy establishes that devices connected to the UC Davis electronic communications network must meet UC Davis security standards or seek exception authorization. Campus units may develop and implement more rigorous security standards. Computing applications hosting critical and/or sensitive university information are subject to more stringent security standards, as defined in UC Business and Finance Bulletin, IS-3.

II. Definitions

- A. Devices--Includes computers, printers, or other network appliances, as well as hardware connected to the campus network from behind security devices/systems.
- B. Additional terms used in this policy are defined in Section 310-23 and 310-24, and UC Business and Finance Bulletin IS-3.

III. Policy

- A. UC Davis security standards (Exhibit A) will be published and maintained by Information and Educational Technology (IET). The standards will be reviewed annually by senior campus administrators and technical representatives.
- B. Campus units must ensure devices connected to the campus network comply with the security standards or develop/implement strategies to mitigate the risks posed by non-compliance.
- C. Campus units must annually report to their respective Dean, Vice Chancellor or Vice Provost, the extent to which unit operations are consistent with the campus security standards. Where compliance is not complete, the report must document a compliance plan, a statement indicating a specific security standard is not applicable or an acknowledgement and acceptance of the information risks associated with continued non-compliance to the security standard. These reports will be summarized by the Deans, Vice Chancellors and Vice Provosts and submitted annually to the Offices of the Chancellor and Provost. The reports will be used to prepare a campus-wide annual report describing the state of UC Davis computing and network security.

IV. Responsibilities

- A. Information and Educational Technology is responsible for
 - 1. developing and publishing security standards.
 - 2. providing guidance on application of security standards.
 - 3. recommending risk assessment tools in support of the security standards.
 - 4. preparing state of security report to the Offices of the Chancellor and Provost.
- B. Campus units are responsible for
 - 1. developing and implementing measures to ensure campus network connected devices are in compliance with security standards.

2. reviewing unit compliance to security standards and prepare and submit annual unit compliance reports/plans to campus administrative officials.
 3. facilitating security training for users, system administrators and managers.
- C. Campus Administrative Officials are responsible for
1. approving security standards.
 2. approving exceptions to security standards.
 3. submitting annual compliance status reports to the Offices of the Chancellor and Provost.

V. Resources and References

- A. Information Security Web Site, (<http://security.ucdavis.edu>), includes report template, tools, reference.
- B. UC Business and Finance Bulletin IS-3, Electronic Information Security.
- C. UCD Policy and Procedure Manual:
 1. Section 310-21, Computer Vulnerability Scanning Policy.
 2. Section 310-23, Electronic Communications--Allowable Use.
 3. Section 310-24, Electronic Communications--Privacy and Access.