

UC Davis Policy and Procedure Manual

Chapter 310, Communications and Technology

Section 21, Computer Vulnerability Scanning Policy

Date: 9/17/04

Supersedes: New

Responsible Department: Information and Educational Technology

Source Document: N/A

I. Purpose and Scope

This policy establishes that computers, servers, and other devices connected to the campus network will be free of critical security vulnerabilities. This policy applies to all users of the UC Davis computing network.

II. Definitions

The UC Davis Electronic Communications Policy (Section 310-16) defines terms used in this policy. Some additional terms are defined here.

- A. Critical security vulnerability--those security vulnerabilities that typically affect default installations of very widely deployed software, resulting in the compromise of servers or standalone computers, and the information required for exploitation (such as sample exploit code) is widely available to attackers.
- B. Timely manner--time response as determined by the nature of the threat in respect to potential damage, known credibility of threat and reported spread.

III. Policy

- A. All computers, servers, and other electronic devices connected to the campus network shall be kept free of critical security vulnerabilities.
- B. Individuals whose computers present critical security vulnerabilities must correct those vulnerabilities in a timely manner before connecting to the campus network.
- C. Computers found to contain critical security vulnerabilities that threaten the integrity or performance of campus network will be denied access to campus computing resources, and may be disconnected from the campus network to prevent further dissemination of infectious or malicious network activity.

IV. Responsibilities

- A. Users must operate computers free of critical operating system and application security vulnerabilities. Those vulnerabilities must be removed or bypassed before accessing the campus computing network.
- B. Information and Educational Technology (IET) will develop, administer, and maintain systems to identify computers with critical security vulnerabilities connected to the UC Davis computing network, notify computer administrators/operators of vulnerabilities and publish vulnerability identification and removal guidance. In addition, IET will publish vulnerability scanning results, and develop, administer, and maintain systems to maintain the integrity and/or performance of the campus computing network.

- C. Vice Provost--Information and Educational Technology or delegate will approve updates of vulnerability scanning systems. These systems will be used to identify computers with critical security vulnerabilities that represent a significant threat to campus computing systems and network.
- D. Campus units will review vulnerability scan reports and remove/bypass critical security vulnerabilities. Campus units will also either conduct independent scans for critical security vulnerabilities within each unit's virtual local area network (VLAN) or permit centrally administered vulnerability scans to transit in/out of the campus unit VLAN. Campus units must control levels of harmful and/or infected network traffic exiting from their VLAN.

V. References and Resources

- A. Section 310-16, Electronic Communications Policy.
- B. Instructional material to remove or bypass critical security vulnerabilities:
<http://security.ucdavis.edu>.