

UC Davis: Offices of the Chancellor and Provost

May 11, 2005

DEANS, DIRECTORS, DEPARTMENT CHAIRS, AND ADMINISTRATIVE OFFICERS

RE: UC DAVIS CYBER-SAFETY PROGRAM

An important new security policy has been officially adopted that will provide our students, faculty, and staff with a much more stable, reliable, and productive environment in which to teach, learn, and conduct research. Named the Cyber-Safety Program, the policy (PPM 310-20) defines both responsibilities and key practices for assuring the integrity, availability and confidentiality of UC Davis computing systems and electronic data. The program also requires annual reporting of how well campus units are progressing to implement the recommended security measures.

Given recent personal information security breaches reported around the nation and here on campus, your active and ongoing participation in the Cyber-Safety Program will be critical to our success. This policy is indeed an essential strategy for improving the UC Davis electronic work environment.

We have attached the action plan that has been discussed with various campus constituencies. The action plan includes some background information as well as the timetable for the production, submission, and review of units' assessment plans and reports.

Thank you for your prompt attention to this memorandum. We appreciate your collaboration in our efforts to protect the integrity, availability, and confidentiality of UC Davis resources.

To access the policy and standards, see <http://manuals.ucdavis.edu/ppm/310/310-22.htm>. If you have questions regarding the Cyber-Safety Program or this directive, please contact Bob Ono, at (530) 757-5795 or raono@ucdavis.edu.

Virginia Hinshaw
Provost and Executive Vice Chancellor

Peter Yellowlees, MBBS, MD
Interim Vice Provost
Information and Educational Technology

UC DAVIS CYBER-SAFETY PROGRAM ACTION PLAN AT A GLANCE

BACKGROUND:

- IT security standards were discussed with Council of Deans and Vice Chancellors, Academic Senate, Senior Advisors, Technology Infrastructure Forum, and Technology Support Program (winter & early spring 2005).
- Based on feedback received, IET moved forward with the policy, established the UC Davis Cyber-Safety Program, and in collaboration with Internal Audit developed a more aggressive timeframe.
- In summary, the policy:
 - Defines responsibilities and 14 key practices for assuring the integrity, availability and confidentiality of UC Davis computing systems and electronic data.
 - Requires annual reporting of how well campus units are progressing to implement the recommended security measures.
 - Was adopted into the campus Policy and Procedure Manual on 4/25/05 (see <http://manuals.ucdavis.edu/ppm/310/310-22.htm>).
- The Program is an essential strategy for improving the campus electronic work environment.

TIMETABLE:

A three-phase approach has been developed. Deadlines and key components:

- **July 1, 2005: Preliminary reporting information**
 - Identification of the individual assigned to lead the assessment and report preparation for the respective school, college or administrative organization and the units to be covered in the organizational plan.
 - Projected target date for security assessment completion.
 - Identification of any additional resources organizations might need to complete the security assessment and report.
- **October 1, 2005: Security assessment plans and status reports**
 - Extent to which units comply with the 14 Cyber-safety standards.
 - Action plan for compliance. Includes projected completion date (for units that have not completed their security assessment), resources needed to complete the assessment, and any other hurdles preventing completion of the unit report.
- **July 1, 2006 (and annually thereafter): Annual IT security reports**

REPORT SUBMISSION AND REVIEW:

- Deans, vice chancellors and vice provosts should submit one consolidated report for their respective organizations.
- Plans and reports should be submitted to Bob Ono, IT Security Coordinator.
- Security assessment plans and status reports will be reviewed by IET and Internal Audit.
- Campus-wide status reports will be presented periodically to CODVC.

RESOURCES:

- IET and Internal Audit are collaborating to:
 - Develop a pool of technical resources to assist deans, vice provosts or vice chancellors who indicate they do not have the resources available to complete the initial assessment and/or correct deficiencies.
 - Structure a consistent review of plans and assessment reports, and to determine the reasonableness of timelines proposed by units to correct deficiencies.
- UC Davis Cyber-Safety Program Web site: <http://security.ucdavis.edu/cybersafety.cfm> (incl. standards, reporting template, tools, additional references)
- Questions about the Program or directive: Bob Ono (757-5795, raono@ucdavis.edu).