




CALIFORNIA STATE UNIVERSITY, LONG BEACH

DIVISION OF ADMINISTRATION AND FINANCE

MEMORANDUM

TO: Campus Community
FROM: William H. Griffith 
DATE: January 22, 2007

As we begin the new semester, it is a good time for each of us to be reminded of our obligation to protect the security and confidentiality of data and information that we work with daily to perform our job responsibilities. Such data and information include records of our students, faculty, staff and customers which contain personal information such as the individual's social security number, home address, home telephone number, and date of birth.

I am sure that many are aware of the recent breach of UCLA's computer files which exposed the records of approximately 800,000 of the university's current and former students, faculty, and staff members, among others. A statement made last week by James Davis, UCLA's Associate Vice Chancellor for information technology suggests that approximate 5% of the individuals whose records were exposed have become victims of identify theft.

While the UCLA information security breach is the largest one known to have occurred at a U.S. college of university, there have been many others in academia in the last few years. Although, there are no comprehensive statistics on computer break-ins at colleges and universities, research revealed that in the first six months of 2006, there were at least 29 security failures at colleges nationwide, jeopardizing the records of 845,000 people. Generally, a breach is the result of lost or stolen electronic equipment or the hacking of a campus computer system.

When a security breach occurs, timely notification to affected individuals may be their best defense against identify theft. The campus has a well developed Security Incident Reporting and Breach Notification Plan to respond promptly and effectively to any security breach. If you believe that a security breach may have occurred, please immediately contact your appropriate administrator, the office of the Vice President for Administration and Finance, extension 55578 and the campus Information Security Officer, extension 58260. After business hours, notification of a suspected or known security breach should be made to University Police, extension 54101.

Continued ...

Protecting our campus' information is one of the campus' strategic goals and is of utmost importance to administrative and information technology personnel. Intrusion protection tools have been deployed on our secure campus network and are continuously monitored. These tools helped protect our campus in 2006 by blocking over 24 million intrusion attacks. Our central administrative systems allow us to stay current on cutting edge technology including the latest security updates to hardware and software.

However, personal and confidential information can be stored throughout the campus in shadow systems, ad-hoc data bases and other electronic or hard copy formats. These systems and records do not share the same level of protection as the central administrative system, and therefore leave the campus vulnerable to security breaches. To address these as well as other related issues, campus policies, procedures, standards, and guidelines are being developed to help us better understand what we must do to prevent the unauthorized disclosure of personal information in our custody and ensure campus compliance with applicable federal and state laws. I look forward to sharing additional information with you in the near future.

In the meantime, remember that information security is everyone's responsibility. The campus Information Security website, http://daf.csulb.edu/offices/vp/information_security/index.html contains useful guidelines for safeguarding personal and confidential information and securing your computer. I urge you to review and follow these guidelines. If each of us takes necessary precautions to protect the personal information maintained in numerous files throughout the campus, we can significantly decrease the chance of a security breach occurring at CSULB.

For additional information regarding information security, please contact Dr. Maryann S. Rozanski, Director, Safety, Risk Management and Information Security at extension 58260 or at mrozansk@csulb.edu.