Memorandum

Office of the Associate Vice Chancellor
Information Technology
MC: 140501

Tél: 310.206.0011
Fax: 310.206.4961

July 3, 2003

VICE CHANCELLORS AND DEANS:


Legislation in California, effective July 1, 2003, adds new sections to the California Information Practices Act requiring notification to California residents regarding any breach to the security of a computing system where there is a reasonable belief that an unauthorized person has acquired their unencrypted personal information. The intent of this legislation is to protect information that could be used, possibly in conjunction with other information, to impersonate an individual in ways that might cause serious loss of privacy and/or financial damage. Protected personal information in this context is narrowly defined as any computerized data containing an individual’s first and last name along with certain common identifiers such as Social Security Number, driver’s license number or bank account number.

The UC Office of the President has issued an amendment to Business and Finance Bulletin IS-3, Electronic Information Security, to address these new legal requirements. My office is coordinating UCLA’s response.

UCLA is implementing these new IS-3 requirements through a draft policy. Though it is still in draft form and will be subjected to the campus review process through the Information Technology Planning Board over the next few weeks, it is important that implementation of some of the requirements begin immediately.

With an expectation that these actions will become part of the permanent campus response once the policy is finalized, we request each Vice Chancellor or Dean to establish processes with which to identify:

- Where personal information is used and stored in the school, division or unit;
- The primary employee positions in the school, division or unit that have access to and use such data;
- The proprietor and/or custodian of such data, if the data is local to the school, division or unit;
A technically acceptable level of security protection for such data. We further request that Vice Chancellors and Deans designate an individual to oversee and ensure compliance with this new policy, and to ensure all suspected security breaches (as defined in the draft policy) within the school, division or unit are investigated. Please provide the names of these individuals to me as soon as practicable. We are requesting a report on these four bullet points by September 30, 2003. Actual or suspected security breaches should be reported to my office immediately.

We wish to call your attention to the stipulation in the draft policy that any financial liability to the University resulting from failure by a unit to comply with this policy shall be assigned to the management unit where the security breach occurred.

For assistance with, or questions about this policy, please contact IT Security and Policy Coordinator Kent Wada (kent@ucla.edu or 6-3874).

Sincerely,

Jim Davis
Associate Vice Chancellor
Information Technology

cc: Executive Vice Chancellor Daniel Neuman
    Administrative Vice Chancellor Peter Blackman
    Directors
    Department Chairs
    Administrative Officers
    Information Technology Planning Board Members
    Common Systems Group