Campus Policy Number: 400-60

Notification of Security Breaches Involving Personal Information

Policy Owner: Computing & Communications
Effective Date: 11/15/2004

I. INTRODUCTION

Senate Bill 1386 and Assembly Bill 700, effective July 1, 2003, added a new provision to the California Information Practices Act - Civil Code 1798.29, 1798.82. This new provision requires any state agency (including the University of California) with computerized data containing personal information to disclose any breach of security of a system containing such data to any California resident whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

The Civil Code defines "personal information" to be an individual's first and last name in combination with any of the following:

- social security number AND/OR,
- driver's license number AND/OR,
- Financial account or credit card number in combination with any password that would permit access to the individual's account.

It requires that owners of computerized data must give notice of any security breach to affected persons in the *most expedient time possible and without unreasonable delay.* The provision also allows for substitute notice (e.g., via posting on the agency's website and notification to major statewide media) in certain circumstances. The bill specifies that an agency that maintains its own notification procedures as part of an information security policy shall be deemed to be in compliance with the bill's notification requirements, as long as the agency notifies people in accordance with its policies in case of a security breach and as long as the agency is otherwise consistent with the bill's timing requirements for notification.

On April 29, 2003 the University of California Office of the President (UCOP) issued an amendment to Business and Finance Bulletin IS-3 - "Electronic Information Security" to address these new legal requirements. The following UCR guidelines and procedures are provided to campus departments and units for their assistance in implementing the UCOP requirements.

II. DEFINITIONS

Protected data.

The data comprising personal information governed by these guidelines is defined as protected data. This protected data includes an individual's first and last name in combination with any of the following:

- social security number AND/OR,
- driver's license number AND/OR,
- financial account or credit card number in combination with any password that would permit access to the individual's financial account.

Computing System.

A computing system is any server, desktop, laptop computer, or PDA (Personal Data Assistant) that contains or provides network access to protected data.

Lead Campus Authority.

The Lead Campus Authority for UCR is the Associate Vice Chancellor for Computing and Communications (C&C). The Lead Campus Authority is responsible for ensuring that the campus incident response process and UCOP (and campus) notification procedures are followed. The Lead Campus Authority will coordinate campus procedures with various campus constituencies (VCA, Audit and Advisory Services, UCR's Locally Designated Official (LDO), UCR's Director of Financial Controls and Accountability, campus counsel, etc.) as appropriate and will maintain as robust a database as possible of campus systems containing protected data.

Responsible Administrative Official *(e.g. Dean, Associate Dean, Vice Chancellor, Assistant Vice Chancellor, etc.)*.

The UCR individual who is ultimately responsible for oversight of data or computing systems within a given functional area.

Data Proprietor *(e.g. MSO, CFAO, Associate Dean, Assistant Vice Chancellor etc.)*.

Data Proprietors are responsible for identifying which computing systems contain protected data or have access to protected data (please see the note below relating to Control Records). They will ensure that appropriate procedures are deployed governing access to protected data and adequate security plans, consistent with Business and Finance Bulletin IS-3, are in place for computing systems within their jurisdiction. Data Proprietors will work with C&C to maintain an inventory of systems containing protected data. An up-to-date systems inventory will usually include the system's location and use, its custodian, and type of security protection. Data Proprietors will inform their Data Custodians, affected staff within their jurisdiction, and third-party users, of University policy and their responsibilities regarding any use they may make of protected data.

Data Custodian *(e.g. Systems Administrator, Database Administrator, etc)*.

Data Custodians are responsible for protecting the resources under their control, such as access passwords, computers, and downloaded data. Contractual arrangements with outside affiliates must include the third-party user's obligations regarding protected data. Data Custodians will ensure implementation of adequate security measures for computing systems containing protected data (e.g. monitoring access logs for computing systems housing protected data can disclose unauthorized access or anomalous activity) as well as appropriate encryption strategies for both the transmission and storage of protected data. Departments may wish to consult with C&C for assistance in determining strategies appropriate to their particular technological environment.

Control Records.

A Control Record is a database, spreadsheet, or any other electronic file containing a list of computing systems that contain protected data. Control records must contain the following:

- name of computing system data custodian,
- physical location of computing system,
- description of logical access and security controls,
- description of protected data stored on the system.

Control Records must be updated and supplied to the Lead Campus Authority at least once per year or at any time a system containing protected data is deployed or significantly modified.

Third-Party User.

A Third Party User is an authorized external contractor or affiliate who uses UCR data containing protected information.

III. INCIDENT RESPONSE PROCESS

1. *INITIAL RESPONSE.* If a breach of security is suspected on a computing system that contains or has network access to unencrypted protected data, the Data Custodian will ***immediately***:

    - Remove the computing system from the campus network.

    - Conduct a local analysis of the breach to determine the number of individuals whose protected data may have been acquired.

    - Notify the Data Proprietor and the Responsible Administrative Official if there is a reasonable belief that protected data may have been acquired, regardless of the quantity of information that might have been compromised.

2. *INITIAL NOTIFICATION OF LEAD CAMPUS AUTHORITY.* If the Data Custodian and Data Proprietor agree that protected data may have been compromised, the Data Proprietor should contact the C&C Network Operations Center at 787-4100 to report that a potential security breach has occurred and to request immediate notification of the Lead Campus Authority. Additional information should be sent via email to security@ucr.edu and the Data Proprietor should quickly contact the appropriate Responsible Administrative Official.

3. *INITIAL ANALYSIS OF SECURITY BREACH.* C&C will examine the evidence of a breach with the Data Custodian to assess the possibility that unencrypted protected data has been acquired by an unauthorized source and report their conclusions to the Lead Campus Authority.

4. *UCOP AND CAMPUS NOTIFICATION OF SECURITY BREACH.* If, after consulting with C&C security staff and the Data Custodian, the Lead Campus Authority is reasonably certain that a security breach has occurred, the Lead Campus Authority will immediately report the breach to the Associate Vice President for Information Resources and Communications at Office of the President as well as the UCR Police Department. Notification will also be sent to UCR's Executive Vice Chancellor and Provost, Vice Chancellor of Administration, Locally Designated Official (see below), and the Responsible Administrative Official.

5. *LOCALLY DESIGNATED OFFICIAL (LDO) NOTIFICATION.* If an improper governmental act is alleged or suspected, as defined in California Government Code Section 8547.2, the Lead Campus Authority will notify the LDO in accordance with Campus Policy Number 650-90 on Reporting and Investigating Allegations of Suspected Improper Governmental Activities.

6. *RECOMMENDATION CONCERNING NOTIFICATION TO INDIVIDUALS IMPACTED BY THE SECURITY BREACH.* The Lead Campus Authority will bring together the appropriate Responsible Administrative Official, Audit and Advisory Services, UCR's Director of Financial Controls and Accountability, and the Vice Chancellor of Administration to make a determination whether criteria for notification under California Civil Code 1798.29, 1798.82 have been met and to determine the means of notification, if such notification is required (e.g., email, postal mail, or website notice, consistent with UCOP Notification Procedures). An incident report and suite of recommendations will be prepared for the Executive Vice Chancellor's review.

7. *NOTIFICATION TO INDIVIDUALS IMPACTED BY THE SECURITY BREACH.* After obtaining the EVC's approval, the Lead Campus Authority will work with the Data Proprietor to ensure that the notification procedure is executed.

IV. BEST PRACTICES RELATING TO SECURING PROTECTED DATA

The University of California has adopted new policies (contained in UC's IS3 security bulletin) aimed at enhancing the management of personal 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. In addition to these new policies (and local UCR procedures to implement this policy), campus departments and units are urged to establish "best practices" to reduce the collection, distribution, and retention of personally identifying electronic data if this data is not critical to their business needs. Such practices should embrace the following concepts:

- Collect and retain only that data which is essential to the performance of assigned tasks.
- Delete personal information when there is no longer a business need for its retention on computing systems.
- Provide staff access to sensitive data only as needed to perform assigned duties.
- Design database systems so that personal information can be identified.
- When personally identifying information is included in the distribution of data to any downstream users, include notification of that fact, including reference to these guidelines.
- Remove personal information not critical to the task when distributing full data sets to downstream users.
- Whenever possible, configure electronic applications that check authorizing or authenticating databases to return confirming responses rather than personal information.
- Review and update agreements with external service providers to ensure vendor compliance with these requirements.
- Be prepared in advance in the event of the need for any immediate notification to individuals whose personal data is retained on computing systems.

- Never leave sensitive data exposed on computer screens when not in use or leave computer screens unattended without appropriate screen access controls.

In addition to these practices, please see C&C's web site http://cnc.ucr.edu/security/index.php relating to server side security and distributed firewalls.

V. REFERENCES

1. California and United States

a. California Civil Code - Sections 1798.29 and 1798.82 (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.25-1798.29) and (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=civ&group=01001-02000&file=1798.80-1798.84)
b. California Information Practices Act of 1977 (IPA) (http://www.privacy.ca.gov/code/ipa.htm)
c. California Public Records Act (CPRA) (http://www.leginfo.ca.gov/cgi-bin/displaycode?section=gov&group=06001-07000&file=6250-6270)
d. Federal Family Educational Rights and Privacy Act of 1974 (FERPA) (http://www.ucop.edu/ucophome/policies/bfb/rmp8.html#IV)
California Department of Consumer Affairs Office of Privacy Protection http://www.privacy.ca.gov/cover/identitytheft.htm
e. Federal Trade Commission's Web site on identity theft
http://www.consumer.gov/idtheft/
f. Social Security Administration fraud line: 1-800-269-0271
g. Credit Bureau Numbers:
Equifax 1-800-525-6285
Experian 1-888-397-3742
Trans Union 1-800-680-7289

2. University of California

h. UCOP Electronic Communications Policy, November 17, 2000 (http://www.ucop.edu/ucophome/policies/ec/)
i. UCOP Policies Applying to Campus Activities, Organizations, and Students, August 1994 (http://www.ucop.edu/ucophome/uwnews/aospol/toc.html)
j. UC Business and Finance Bulletins (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)

k. UCOP IS-3, Electronic Information Security (http://www.ucop.edu/ucophome/policies/bfb/is3toc.html)
l. UCOP IS-10, Systems Development and Maintenance Standards (http://www.ucop.edu/ucophome/policies/bfb/is10.pdf)
m. UCOP RMP-8, Legal Requirements on Privacy of and Access to Information (http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html)
n. UCR Server Side Security and Firewalls (http://cnc.ucr.edu/security/index.php)