UCLA Policy xxx: Notification of Breaches of Computerized Personal Information

Issuing Officer: Associate Vice Chancellor, Information Technology
Responsible Dept: Office of Information Technology
Effective Date: New

I. REFERENCES
1. UC Business and Finance Bulletin, IS-3, Electronic Information Security;
4. Protection of Personal Information, UC Office of the President web site.

II. BACKGROUND
Effective July 1, 2003, a new provision has been added to the Information Practices Act of 1977, codified in California Civil Code, §§1798.29 and 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.

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. This Policy defines local provisions and procedures that implement IS-3 Section IV.D, Notification in Instances of Security Breaches Involving Personal Information Data.

III. PURPOSE
This policy describes the circumstances under which notification of a system Security Breach is required and identifies the Campus Officials responsible for responding to a computer breach to determine if notification, as described above, is required, and for initiating such notification. This policy also describes the responsibilities of Vice Chancellors and Deans for ensuring compliance in their respective units. This policy applies to Personal Information data in electronic form and not to hard copies of same.

IV. DEFINITIONS
Security Breach Coordinator: for purposes of this Policy, the individual or functional position designated by a Vice Chancellor or Dean with overall responsibility in a school, division or unit for ensuring compliance with this Policy.
**Director, Information Technology Policy:** the functional position to which certain duties are delegated by the Associate Vice Chancellor, Information Technology.

**Personal Information:** as used in this policy, an individual’s first name or first initial, and last name, in combination with any one or more of the following: (1) social security number, (2) driver’s license number or California identification card number, or (3) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

**Security Breach:** when unencrypted Personal Information of a California resident is reasonably believed to have been acquired by an unauthorized person. Acquisition of personal information by a University employee or agent for bona fide University business purposes does not constitute a Security Breach, provided that the Personal Information is not further disclosed to an unauthorized person.

**V. STATEMENT**

Each campus must follow the systemwide procedures set forth in Business and Finance Bulletin IS-3 to provide notification of a Security Breach, and develop an implementation plan for such notification, including the designation of a lead campus authority and establishing an incident response process to determine whether a Security Breach has occurred.

**A. Responsibilities and Duties**

1. **Vice Chancellors and Deans**
   
   Vice Chancellors and Deans are responsible for the security of data files containing Personal Information in their respective areas. Accordingly, they must establish processes 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.

   These responsibilities may be delegated to others as appropriate, however ultimate accountability for the security and whereabouts of electronic records containing Personal Information rests with the Vice Chancellor or Dean for their respective areas of responsibility. Any financial liability to the University resulting from failure by a unit to comply with this Policy shall be assigned to the unit where the Security Breach occurred.

   Each Vice Chancellor or Dean must designate a Security Breach Coordinator who will ensure all suspected Security Breaches within the school, division or unit are investigated and actual Security Breaches are reported to the Associate Vice Chancellor, IT.

   Vice Chancellors and Deans are responsible for signing and issuing the written notification of a Security Breach in their respective areas to the affected California resident(s).

2. **Associate Vice Chancellor, Information Technology (IT)**
   
   The Associate Vice Chancellor, IT is responsible for reporting Security Breaches and their ultimate resolution to UCOP and is the designated lead campus authority, in accordance with the implementing guidelines of IS-3. When a Security Breach occurs, the Associate Vice Chancellor, IT reports the incident in writing, to the Associate Vice President for Information Resources and Communications, UC Office of the President. When the incident is closed, notification will again be made, in writing, including the following information:
   
   • A description of the incident
   • The response process
   • The notification process
• The actions taken to prevent further breaches of security.

3. Director, Information Technology (IT) Policy
The Associate Vice Chancellor, IT delegates the following responsibilities to the Director, IT Policy:

• Ensuring that the campus incident response process is followed;
• Ensuring that systemwide and, if applicable, campus notification procedures are followed; and
• Coordinating with appropriate Campus Officials, as noted in V.B. below.

B. Security Breach Incident Response Process
Any instance of a suspected Security Breach should be reported immediately to the appropriate campus authorities, who will follow the incident response process noted below.

<table>
<thead>
<tr>
<th>RESPONSIBILITY</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Breach Coordinator</td>
<td>Ensures that any suspected Security Breaches within their units are investigated. Reports actual Security Breaches to the Associate Vice Chancellor, IT and ensures that appropriate action is taken to secure such breaches expeditiously.</td>
</tr>
</tbody>
</table>
| Associate Vice Chancellor, IT  | • Notifies UCOP in writing (Section V.A).  
                                | • Notifies the Director, IT Policy. |
| Director, IT Policy            | In cooperation with the Security Breach Coordinator, coordinates with:  
                                | • Associate Vice Chancellor, IT, Campus Counsel and UCLA Police as appropriate to confirm the Security Breach; and with  
                                | • Campus Counsel and University Communications to ensure that appropriate notification text is developed (Section V.C). |
| Vice Chancellor or Dean        | Issues notification under his or her name. |
| Associate Vice Chancellor, IT  | Notifies UCOP of final disposition of incident (Section V.A). |

C. Notification Requirements
In the event of a Security Breach, UCLA must provide notification of the breach to those California residents whose Personal Information is reasonably believed to have been acquired by an unauthorized person. Notification must occur without unreasonable delay, except:

• When a law enforcement agency has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the law enforcement agency determines that it will not compromise the investigation), or
• In order to discover the scope of the Breach and restore the integrity of the system.

Appropriate notification will be distributed, in consultation with the Associate Vice Chancellor, IT and Campus Counsel, by written, hard copy or by e-mail and issued by the Dean or Vice Chancellor whose department or unit experienced the Security Breach. If sufficient contact information is not available for direct hard copy or e-mail notice, a substitute method of notice may be used. This substitute method shall be determined by the Associate Vice Chancellor, IT, in consultation with Campus Counsel and the Assistant Vice Chancellor, University Communications, and will include prominent display on the UCLA gateway, www.ucla.edu, for at least forty-five days.

VI. DATA SECURITY GUIDELINES
This policy is intended to enhance the management of Personal Information that could be used, possibly in conjunction with other information, to impersonate an individual in ways that might cause loss of privacy and/or financial damage. Departments are urged to establish best practices to minimize the collection,
distribution, and retention of personally identifying electronic data if this data is not critical to their business needs. Such practices should comply with the following principles:

- 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 this Policy;
- redact 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.

Further information can be found in the Administrative Responsibilities Handbook.

VII. ATTACHMENTS

A. Sample Notification Text (University of California)

http://www.ucop.edu/irc/itsec/samtext.pdf

Issuing Officer

/s/ Jim Davis

Associate Vice Chancellor, Information Technology

Questions concerning this policy or procedure should be referred to the Responsible Department listed at the top of this document.