I. REFERENCES

1. UC Business and Finance Bulletin, IS-3, Electronic Information Security;
4. Protection of Personal Information, iCompass.

II. BACKGROUND AND PURPOSE

Effective July 1, 2003, a provision in the Information Practices Act of 1977, codified in California Civil Code, §§1798.29 and 1798.82, 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. In April, 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 legal requirements.

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

- The circumstances under which notification of a System Security Breach is required;
- The Campus Officials responsible for responding to a computer breach to determine if notification, as described above, is required, and for initiating such notification; and
- The responsibilities of Vice Chancellors and Deans for ensuring compliance in their respective units.

UCLA intends to notify all affected individuals regardless of their place of residency.

This policy applies to Personal Information data in electronic form and not to hard copies of same.

III. DEFINITIONS

**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 an individual 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 or persons.

**Security Breach Coordinator**: for purposes of this Policy, the individual or functional position designated by a Vice Chancellor or Dean to whom Suspected Security Breaches are reported and with overall responsibility for ensuring compliance with this Policy, by his/her respective school, division or unit.

**Suspected Security Breach**: occurs when such a computer or computer device containing Personal Information is, among other possibilities, lost or stolen, accessed in unauthorized fashion or infected by a virus or worm, but it is not yet known whether the Personal Information has been compromised to meet the level of a Security Breach.

**System**: for purposes of this policy, is any computer or computing device, including, but not limited to, desktops, laptops, PDAs, removable media such as CDs, USB flashdrives or iPods used as storage devices.

**IV. 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 and ensure that that individual reads this Policy and understands his/her responsibilities thereof.

   Vice Chancellors and Deans shall be responsible for any costs associated with notification of a Security Breach in their respective areas.

2. **Security Breach Coordinators**
   Security Breach Coordinators are responsible for:
• Ensuring that all Suspected Security Breaches within their respective school, division or unit are investigated and reported to the Associate Vice Chancellor, IT.

• Acting as liaison between their respective school, division or unit and the Director, IT Policy to facilitate investigation of such Suspected Security Breaches.

• Making arrangements for implementing notification requirements, including the actual distribution of notification letters or emails and the setting up of a hotline for inquiries if appropriate.

Other related duties and responsibilities may be assigned to a Security Breach Coordinator as deemed necessary by his/her respective Vice Chancellor or Dean.

3. **Associate Vice Chancellor, Information Technology (IT)**

The Associate Vice Chancellor, IT is the designated lead campus authority, in accordance with the implementing guidelines of IS-3, and is responsible for:

• Reporting all confirmed Security Breach incidents, in writing, to the Associate Vice President for Information Resources and Communications, UC Office of the President (UCOP), and their ultimate resolution (see section IV.C below).

• Making a final determination as to whether notification of a Suspected Security Breach is warranted, based on the recommendation from the Director, IT Policy, as noted in section IV.B and IV.C below.

• As appropriate, may also report Suspected Security Breaches to UCOP where a decision has been made not to notify.

4. **Director, Information Technology (IT) Policy**

The Associate Vice Chancellor, IT delegates the following responsibilities to the Director, IT Policy:

• Ensuring that the campus Security Breach incident response process is followed (see IV.C below);

• Ensuring that systemwide and, if applicable, campus notification procedures are followed; and

• Coordinating with appropriate Campus Officials, as noted in IV.C. below, to analyze and recommend, in writing, to the Associate Vice Chancellor, IT, whether a Suspected Security Breach warrants notification or not.

**B. Notification Requirements**

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

• When the UCLA Police has determined that notification will impede a criminal investigation (in this case, notification must occur as soon as the UCLA Police determines that it will not compromise the investigation), or

• In order to discover the scope of the Security Breach and restore the integrity of the System.

In coordination with Campus Counsel, appropriate notification for each incident will be composed and distributed by written hard copy or by e-mail. A determination will be made as to which Campus Official is most appropriate to sign the notification.

If sufficient contact information is not available for direct hard copy or e-mail notice, a substitute method of notice will be determined.
C. Security Breach Incident Response Process

Any instance of a Suspected Security Breach must be reported immediately to the appropriate Security Breach Coordinator (see Attachment A), who will initiate the incident response process described below.

1. Initial Reporting and Analysis

<table>
<thead>
<tr>
<th>RESPONSIBILITY</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Breach Coordinator</td>
<td>When notified of a Suspected Security Breach, ensures that appropriate action is expeditiously taken to secure the affected System.</td>
</tr>
<tr>
<td></td>
<td>Immediately notifies the Associate Vice Chancellor, IT.</td>
</tr>
<tr>
<td></td>
<td>Files a report with the UCLA Police if criminal activity is suspected to be responsible for the Security Breach.</td>
</tr>
<tr>
<td>Associate Vice Chancellor, IT</td>
<td>Notifies UCOP in writing (Section IV.A.3).</td>
</tr>
<tr>
<td></td>
<td>Notifies the Director, IT Policy.</td>
</tr>
<tr>
<td>Director, IT Policy</td>
<td>In conjunction with the Security Breach Coordinator:</td>
</tr>
<tr>
<td></td>
<td>• Works with appropriate technical staff to complete technical analysis of the affected System.</td>
</tr>
<tr>
<td></td>
<td>• Works with Campus Counsel and/or UCLA Police as appropriate to recommend to the Associate Vice Chancellor, IT, as to whether this is an actual Security Breach or not. The analysis leading to the recommendation shall be documented in writing.</td>
</tr>
<tr>
<td>Associate Vice Chancellor, IT</td>
<td>Based on the recommendation from the Director, IT Policy, makes a final determination as to whether this is a notifiable Security Breach or not.</td>
</tr>
</tbody>
</table>

2. Security Breach Notification

<table>
<thead>
<tr>
<th>RESPONSIBILITY</th>
<th>ACTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Breach Coordinator</td>
<td>In conjunction with the Director, IT Policy, works with the Assistant Vice Chancellor, University Communications and Campus Counsel to:</td>
</tr>
<tr>
<td></td>
<td>• Develop an appropriate notification letter (Section IV.B).</td>
</tr>
<tr>
<td></td>
<td>• Determine a substitute method of notice if sufficient contact information is not available for direct hard copy or email notice.</td>
</tr>
<tr>
<td>Associate Vice Chancellor, IT</td>
<td>In consultation with the Assistant Vice Chancellor, University Communications, Campus Counsel and the Dean or Vice Chancellor whose department or unit experienced the Security Breach, determines the most appropriate Campus Official to sign the notification letter.</td>
</tr>
<tr>
<td>Security Breach Coordinator</td>
<td>Arranges for the logistics to implement notification (Section IV.B).</td>
</tr>
</tbody>
</table>

The Associate Vice Chancellor, IT will notify UCOP of the final disposition of the Security Breach incident, including a description of the incident, the response process, the notification process, and the actions taken to prevent further breaches of security.

V. ATTACHMENTS

A. List of Campus Security Breach Coordinators (as of xx/xx/xx)
B. Data Security Guidelines
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.
ATTACHMENT A

List of Campus Security Breach Coordinators (as of xx/xx/xxxx)
ATTACHMENT B

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.