UCSD Implementation Plan
For Protection of
Electronic Personal Identity Information

September 10, 2003

TABLE OF CONTENTS

I.   Overview

The purpose of this plan is to outline procedures for management of all electronic 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. Departments that manage activities that require collection or management of specific "personal identity information" (PII) must protect such data appropriately and also must report any compromise of that protection to affected subjects of that data.

These procedures are intended to comply with the legislative requirements of California Civil Code Sections 1798.82 and 1798.29 or the portions of the California Information Practices Act signed into law in September 2002, and effective July 1, 2003. These procedures augment some of the responsibilities as defined in "Business & Finance Bulletin IS-3: Electronic Information Security."[1]

II.   Definitions

Certain terms used within these procedures are to be interpreted with the following meanings.

A.   Breach of Security

A breach of security occurs when unauthorized access to a system occurs or is reasonably believed to have occurred, and which would have offered the perpetrator an opportunity to acquire electronic personal identity information in unencrypted form.

B.   Electronic Personal Identity Information (electronic PII)

Electronic personal identity information (electronic PII) is the electronic manifestation of an individual's first name or initial, and last name, in combination with one or more of the following:
a) Social Security number (SSN).
b) Drivers license number or State-issued Identification Card number.
c) Account number[2], credit card number, or debit card number in combination with any required security code, access code, or password such as expiration date or "mother's maiden name" that could permit access to an individual's financial account.

This definition of electronic PII is not dependent on where the personal identity information is stored. This includes, but is not limited to, formal database systems such as DB2, Sybase, or Oracle as well as simple text files, spreadsheets, etc. Electronic personal identity information may exist on, but is not limited to, hard drives, magnetic tape, optical disks, diskettes, hand held computing devices, etc.

C.   Encryption

To alter data so as to be unintelligible to unauthorized parties.

---

[1] See BFB, IS-3 http://www.ucop.edu/ucophome/policies/bfb/is3.pdf
[2] "Account number" is not defined in the legislation but can refer to any financial account such as a bank or brokerage account, etc

D.   Unencrypted

Unencrypted data is called *plain or clear text*.

E.   System Administrator

(Also known as the **Electronic Information Resource Custodian**[3]): The department or individual that has physical or logistical control over the Electronic Information Resource.

F.   Subject

Individual to whom the electronic PII pertains.

G.   System

(Also known as **Electronic Information Resource[4]**) A system is any computer readable collection of information that contains electronic personal identity information in an organized form such that information about a particular individual can be distinguished from information about other individuals.

H.   Data Steward

(Also known as the **Electronic Information Resource Proprietor[5]):** The steward of a system is the individual designated by the Chancellor or his or her designee as having the responsibility for determining the purpose and function of the Electronic Information Resource. This can be, but is not limited to, the operating head of a unit or a delegate. Such responsibility may include, for example: specifying the uses for a departmentally-owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which users may have access to an application or to data accessible via an application. All electronic information resources are University resources, and Electronic Information Resource Proprietors are responsible for ensuring that these resources are used in ways consistent with the mission of the University as a whole.

III.   *Areas of Responsibility*

A.   Computing Services[6]

The Director of Academic Computing Services has been designated by the Chancellor as the lead campus authority, having the following responsibilities under these procedures:
- Ensuring that the campus incident response process is followed.
- Ensuring that system-wide and campus notification procedures are followed.
- Coordinating campus procedures with General Counsel and other members of the Computer Incident Response Team.
- Providing initial and closing reports to University of California, Office of the President (UCOP).

---

[3] See BFB, IS-3 http://www.ucop.edu/ucophome/policies/bfb/is3.pdf, section IX(C) "Electronic Information Resource Proprietor, Custodian and User Responsibilities"
[4] ibid
[5] ibid
[6] Joint activity between Academic Computing Services and Administrative Computing and Telecommunications

B.   Data Steward

This person is the person or office responsible for the collection and use of electronic PII, for ensuring that the information is protected adequately, and for determining who should have access to it. The Data Steward may delegate the role to a manager within the same department.

Each Data Steward has the following responsibilities under these procedures:
- Inventory all systems under their control containing electronic PII via online inventory form, including updating information as necessary.
- Ensure appropriate measures and checks are in place for protection of electronic PII under their control, including any downloading of such information.
- Ensure that these procedures are followed for all breaches of systems under their management containing electronic PII.
- Submit initial and closure breach reports to the Computer Incident Response Team.
- Participate in notification as requested by the Computer Incident Response Team.
- May delegate operational management of the electronic personal identity information to a System Administrator.

C.   System Administrator

This person might be a different person or office from the Data Steward and is responsible for regular operational support, backup, and system maintenance of a system with electronic PII.

Each System Administrator has the following responsibilities under these procedures:
- Provide ongoing protection of electronic PII.
- Alert Data Steward, Information Systems Security Team (ISST) (security@UCSD.edu) of possible security breaches.
- Work with ISST to restore system integrity and provide information about the breach and scope.

D.   Information Systems Security Team (ISST)

This team is composed of ACT Data Security & ACS/Network Security staff members (security@UCSD.edu). They will have the following responsibilities under these procedures:
- Confirm that a security breach of unencrypted electronic PII has taken place.
- Work with the system administrator to resolve the security breach.

E.   Computer Incident Response Team (CIRT)

Campus units have responsibilities within these procedures as members of the Computer Incident Response Team (CIRT). The ongoing team members of this group include; ACS Director, ACT Data Center Director, Network Security Manager, and Data Security Manager, and as required, the Data Steward. This team ensures the completion of notification procedures. Other areas listed below will be brought into the process as needed.

CIRT:
- Determine that the criteria for notification have been met.

- Develop notification plan.

UCSD Police Department (Law Enforcement):
- Advise if criteria for notification have been met.
- Authorize that proceeding with notification will not impede a criminal investigation.
- Advise and review means and text of notification.

Office of General Counsel (OGC):
- Advise if criteria for notification have been met.
- Advise, review and approve means and text of notification.
- Provide other legal advice as requested or required.

Public Information Office (PIO):
- Advise and review means and text of notification.
- Perform notification to affected individuals

Internal Audit:
- Advise if criteria for notification have been met.
- Advise and review means and text of notification.

IV. Procedures

A. Electronic Personal Identity Information to Protect

All electronic PII must be managed according to the procedures in this document. If unencrypted electronic PII is reasonably believed to have been acquired by an unauthorized person, state law requires notification to subjects.

These procedures are required of any Data Steward that is responsible for electronic PII. Systems containing electronic PII are also subject to the broader requirements of "Business & Finance Bulletin IS-3: Electronic Information Security."[7]

B. Electronic Personal Identity Information Management Procedures

1. Inventory

Data Stewards with primary responsibility for the existence of electronic PII must maintain an inventory of all systems containing that electronic data. The Data Steward conveys this inventory to the CIRT via an online form located at **https://a4-devqa.ucsd.edu/privatedatareg**. Registration will consist of identifying PII elements stored, the computing system on which they are stored, and contact information for the responsible Data Steward and System Administrator.

Any new systems or systems enhancements that newly qualify an existing system for these guidelines must be added to that inventory as soon as possible.

Please refer to Appendix A for the specific information collected as part of the inventory.

---

[7] See BFB, IS-3: http://www.ucop.edu/ucophome/policies/bfb/is3.pdf

On or before June 30 of each year, the inventory for each department shall be reviewed by the relevant Data Steward and its accuracy as of June 1 confirmed in writing (or via email) by the department head to the CIRT.

2. Electronic Personal Identity Information Protection

Data Stewards must ensure appropriate measures and checks are in place for protection of electronic PII. Although information might be encrypted, replicate information may exist unencrypted occasionally which, if compromised, would result in a required notification. Therefore, reasonable precautions should be in place to protect such unencrypted information including any downloading of such information or temporary storage on other systems.

A person downloading data temporarily assumes the role and responsibilities of Data Steward for the protection of that data and would be required to work with the CIRT team should notification to subjects be required due to an event of unauthorized access.

Email that contains PII must be treated with care and should not be preserved any longer than absolutely necessary.

Data Stewards must also follow other legal and institutional requirements for protection of sensitive electronic PII.[8] If there is any question about the adequacy of current controls, a review by the UCSD CIRT (ucsd-cirt@ucsd.edu) or UCSD Internal Audit staff should be requested.

3. Contact Information

Individuals may need to be notified of an actual or reasonably suspected breach of a system containing electronic PII. Where possible, the primary source of data or office of record should maintain contact information for each relevant individual or must have a plan for substitute notice consistent with the legislation for informing individuals of breaches of security.

Contact information should include the subject's email address, if available. It should include the subject's primary U.S. postal address whenever possible as well. Contact information does not need to be stored with the electronic PII.

Contact information must be valid and current.

C. Breach of Security Procedures

1. Suspected Breaches

Any suspected breaches of a system containing electronic PII must be reported to security@UCSD.edu regardless of how the suspicion arose. ISST in partnership with the System Administrator will confirm the security breach of unencrypted electronic PII.

---

[8] See References

A confirmed security breach must be brought to the attention of the Data Steward. The Data Steward may file a police report with the UCSD Police Department if criminal activity is suspected.

2. Incident Response

The incident response process is initiated with a confirmed security breach of unencrypted electronic PII. The Data Steward must complete the Initial Report (Appendix B), and submit this to the CIRT as the campus Designated Authority as soon as possible, but no later than 24 hours after the breach has been discovered.

Based on the Data Steward's Initial Report, the CIRT will file an initial report of the breach to the Associate Vice President for Information Resources and Communications at UCOP.

The CIRT will convene to determine whether criteria for notification have been met.

ISST and the System Administrator work together to restore the service and integrity of the system with appropriate documentation and preservation of evidence.

Upon resolution of the breach, the Data Steward (or designee) must complete the Final Report (Appendix C), and submit this to the CIRT as the campus Designated Authority as soon as possible, but no later than 24 hours after the situation has been resolved.

Law enforcement must be consulted to ensure that notification will not impede a criminal investigation.

3. Notification Procedures

The Final Report from the Data Steward and the authorization from Law Enforcement initiate the notification procedures.

The Computer Incident Response Team determines the notification plan, including the means and text of notification. Sample language is included as Appendix E.

Upon approval of the notification plan by the General Counsel, the CIRT works with the Public Information Office to deliver the notification. The CIRT will work with the Data Steward as required for additional advice or assistance to affected individuals.

4. Reporting Procedures

The CIRT will submit a Closure Report (Appendix D) to the Associate Vice President for Information Resources and Communications at UCOP as soon as the subject notification process is completed, or if any problem is encountered during that process. This report should detail the nature and cause of the incident, what notification was done and to whom, and what steps have been taken to prevent a recurrence of such an incident.

V. Getting Help

Internal Audit is available to assist with compliance controls and procedures.

Questions on policies and related procedures may be directed to the Computing Policy Officer (computingpolicies@ucsd.edu)

VI. Applicability and Authority

Jurisdiction of this Implementation Plan is under the auspices of Academic Computing Services (ACS) and Administrative Computing and Telecommunications (ACT). Questions concerning this policy should be referred to computingpolicies@ucsd.edu.

This Plan applies to all campus units which maintain electronic PII. Under the terms of the law, any third-party use of University-owned electronic PII is also governed by this Plan, and UCSD must be notified when a breach of security is believed to have put University-owned data at risk. All third-party contracts or agreements should contain language to the effect that they understand our requirements for protection of this type of data.

References

Federal Statutes

Federal Family Educational Rights and Privacy Act of 1974, dated July 17, 1976 (20 U.S.C. Section 1232g)
http://www.ed.gov/offices/OM/fpco/ferpa/

Federal Privacy Act of 1974 - Public Law 93-579 (5 U.S.C. 552a)
http://www.usdoj.gov/foia/privstat.htm

State of California Statutes

State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)
http://www.privacy.ca.gov/ipa.htm

State of California Public Records Act (Gov. Code Section 6250 et seq.)

University of California

University of California Policies
http://www.ucop.edu/ucophome/coordrev/ucpolicies/

University of California Business and Finance Bulletins
- UC-BFB A Series - Accounting
- UC-BFB BUS Series - Business Affairs
- UC-BFB G Series - General
- UC-BFB IA Series - Internal Audit
- UC-BFB IS Series - Information Systems
- UC-BFB PM Series - Physical Plant Management
- UC-BFB RMP Series - Records Management

University of California, San Diego

UCSD – Official Policies and Procedures
http://adminrecords.ucsd.edu/index.html

UCSD Administrative Computing & Telecommunications
http://www-act.ucsd.edu/

UCSD Academic Computing Services
http://www-acs.ucsd.edu/

Network Security Policy
http://adminrecords.ucsd.edu/PPM/docs/135-3.HTML

Administrative Records Identity Theft Notices
http:adminrecords.ucsd.edu/notices/2003/index.html

UCSD Administrative Computing Security
http://blink/go/security

Appendix A
Information Collected via Online Inventory
(https://a4-devqa.ucsd.edu/privatedatareg)

Appendix B

Data Steward INITIAL Report

To be submitted by Data Steward to UCSD CIRT as soon as possible, but no later than 24 hours after breach is *discovered*.

UCSD Computer Security Incident Report
Reporter's contact information
Name: Department:
Email address: Phone number:
Date of report:
Date of incident:
Machine name: Machine IP address:
Was physical media involved?   yes no
SB1386 personal information present: yes no
If yes, which?   SSN yes/no   Driver's License yes/no   Credit card yes/no
Description of incident:
How was incident discovered?
What steps were taken after discovery?
Is further investigation warranted?   yes no
Other agencies contacted about this incident (police, FBI, etc):
Rec'd by   on
V .01

Portions of this report will be included in the CIRT's Initial report to UCOP.

Appendix C

CIRT FINAL Report

To be submitted by CIRT to the UCSD CIRT as soon as possible, but no later than 24 hours after breach is **resolved**.

Scope of breach	
Source of breach	
Description of data compromised	
Population	
Actions taken to prevent further breaches of security	
Time to resolve breach	

Portions of this report will be included in the CIRT's Closure report to UCOP.

Appendix D

CIRT Closure Report to UCOP

Description of the incident	
The response process	
The notification process	
Actions taken to prevent further breaches of security	

Appendix E

Sample Notification Text

University wide requirements for notification of individuals when their personal data has been acquired by an unauthorized individual through a security breach are found in Business and Finance Bulletin, IS-3, Section IV.D, "Electronic Information Security."

The following text is intended to provide guidance in developing a notice to subjects of a database compromise. The final text that is used in any actual breach notification should be reviewed by the Office of General Counsel.

To Whom It May Concern:

This message is being sent to you as a formal notice that personal information relating to you, and maintained in a University of California electronic information system, may have been compromised by a recent security breach. This notification constitutes the notification required pursuant to California Civil Code Section 1798.29.

The personal information which may have been obtained by an unauthorized person was contained in [*name/function of database*] and consisted of the following items of personal information: [*list data elements*].

The possible security breach consisted of [*non-technical description of scope and nature of breach, likelihood of information having been copied, etc.*].

Possible use of this information by the unauthorized person(s) might result in financial loss to you. If this is of concern, please seek advice from your bank or financial advisor. In addition, information at the following web sites might prove helpful:

- http://caag.state.ca.us/idtheft/tips.htm
- http://www.dmv.ca.gov/consumer/fraud.htm

The University has taken immediate steps to prevent a recurrence of this possible breach of security, and is investigating the possible breach for purposes of pursuing action against the individual(s) responsible, as well as finding out additional information regarding the extent to which personal information in the database was actually compromised. If you have any questions about this matter, please contact: [*insert appropriate contact person*]