

UCSC Implementation Plan for Protection of Electronic Restricted Data

Originally *UCSC Implementation Plan for Protection of Electronic Personal Identity Information*, June 26, 2003

Updated May 2008

Table of Contents

Law and University Policy	1
UCSC Implementation Plan	1
I. Scope	1
II. Applicability	2
III. Definitions	2
IV. Management and Protection of Electronic Restricted Data	2
V. Personal Identity Information (PII) Inventory	3
VI. Security Breach Procedures.....	4
VII. Responsibilities and Authority	7
VIII. Contact Information and Getting Help.....	10
IX. Related Policies / References for More Information.....	10
X. Appendices	12

Law and University Policy

These procedures are intended to comply with the legislative requirements of California Civil Code Sections 1798.29 and 1798.82, the portions of the California Information Practices Act signed into law in September 2002, and effective July 1, 2003, and incident response requirements under Federal HIPAA legislation, the Payment Card Industry Data Security Standard, and *UC Business & Finance Bulletin IS-3: Electronic Information Security*¹. These procedures also augment some of the responsibilities defined in IS-3.

UCSC Implementation Plan

I. Scope

This Implementation Plan outlines procedures relating to security breaches, suspected security breaches, and management of “personal identity information” (PII) and other types of electronic restricted data, i.e. data whose unauthorized access might cause serious loss of privacy and/or financial damage, including electronic protected health information (ePHI) protected by Federal HIPAA legislation, credit card data regulated by

¹ See References for all listed laws and policies.

the Payment Card Industry (PCI), and student records protected by the Federal Family Educational Rights and Privacy Act of 1974 (FERPA).²

II. Applicability

These procedures apply to all campus units as well as to those organizations and agencies, public and private, which conduct business or have other electronic information interactions with UCSC.

These procedures amend and supercede the *UCSC Implementation Plan for Protection of Electronic Personal Identity Information*, published June 26, 2003.

III. Definitions

The following terms used in these procedures are defined in the online *Glossary of selected terms in UCSC IT-related policies, procedures and guidelines*, available at <http://its.ucsc.edu/security/policies/glossary.php>.

- Breach of Security
- Electronic Personal Identity Information (PII)
- Electronic Protected Health Information
- Encryption
- Payment Card Industry
- Primary Service Provider
- Restricted Data
- Service Provider
- Student Records Protected by FERPA (FERPA-protected data)
- System
- System Steward

Additional definitions:

Subject: The individual to whom the electronic restricted data pertains.

IV. Management and Protection of Electronic Restricted Data

All individuals are responsible for the appropriate protection of restricted data under their jurisdiction or control.

General practices for the protection and management of electronic restricted data are available on the ITS Security website at <http://its.ucsc.edu/security/policies/rd.php>. Online computer security awareness training is also available.³ Systems containing

² See References

³ http://its.ucsc.edu/security_awareness/training.php

electronic PII and other restricted data are also subject to the broader requirements of IS-3 and other legal and institutional requirements for protection of this data.⁴

Specific System Steward, Service Provider, and Management Responsibilities

- **System Stewards** are responsible for identifying restricted data under their purview and communicating this information, along with associated information about appropriate access and use, degree of sensitivity, criticality, and risk tolerance, to Management and Service Providers.
- **Service Providers** are responsible for understanding the above information from System Stewards and for ensuring the appropriate protection of restricted data on systems under their control, including any downloading of such information or temporary storage on other systems.
- **Management** is responsible for understanding the above information from System Stewards and for ensuring that individuals have appropriate authorization and user and security training prior to accessing restricted data.

If there is any question about the adequacy of current controls, a review by the UCSC Information Systems Security Team (UCSC Security Team) or UCSC Internal Audit staff should be requested.

V. *Personal Identity Information (PII) Inventory*

IS-3 requires campuses to establish a process or processes to identify

- where PII is used and stored,
- the primary employee positions that have access to and use of the data,
- the System Steward and Primary Service Provider of the data, and
- an acceptable level of security protection for the data (addressed in Section IV, above).

UCSC has adopted a three-tiered approach to establish and maintain this inventory:

1. Identify locations where PII is likely to be used and stored, including employee types or classes that have access to and use of the data, and the original source of the PII – these “likely locations” also suggest questions that can be asked in determining whether a breached system is likely to have contained PII;
 - These patterns are identified in conjunction with ITS Divisional Liaisons (DLs) and Applications Solutions.
 - DLs and ITS Directors are responsible for assessing classes of systems under their purview that are likely to contain PII, and for assessing the likelihood that a compromised system may contain PII.
2. Identify known central source systems containing PII, including System Steward, Data Integrator, if applicable, and Responsible Service Provider;

⁴ See http://its.ucsc.edu/security_awareness/restricted_data_resources.php for information and tools.

- The Director, ITS Applications Solutions, is responsible for developing and maintaining this inventory.
3. Establish triggers for checking systems for PII and removing it when possible.
- Triggers are established in conjunction with DLs and appropriate ITS Directors and include
 - a. re-purposing/re-assigning a computer,
 - b. transferring files from an old computer to a replacement computer,
 - c. DL/Local IT Specialist acquiring a new server to support or manage,
 - d. new server going into the ITS Data Center,
 - e. equipment or media disposal.
 - f. when an individual changes jobs and takes their files with them
 - Service Providers are responsible for performing system review according to established triggers, as well as for reviewing results with the owner of the data.
 - Where PII is identified and must be retained, the Service Provider shall work with the IT Service Manager for Community and Compliance to update the inventory in item 1 of this section, above.

VI. Security Breach Procedures

A. Reporting Suspected Breaches.

Any suspected security breach of electronic Personal Identity Information (PII) or other restricted data whose unauthorized access might cause serious loss of privacy and/or financial damage must be reported to the ITS Support Center or UCSC Security Team regardless of how the suspicion arose. The ITS Support Center will escalate reports to the UCSC Security Team. The UCSC Security Team, in partnership with the Service Provider, will confirm the security breach of unencrypted electronic PII or electronic restricted data. If no one is available to receive a report, individuals may contact ITS Security directly. Individuals should also inform their supervisor or appropriate management of possible security breaches involving restricted data.

Any suspected theft of UCSC-related computing equipment should be reported to the UCSC Police Department. The report should include whether the stolen equipment contains any restricted data, including PII. Local authorities should also be contacted for incidents occurring away from campus.

Service Providers, System Stewards, Unit/Departmental Managers, and Deans are also to report suspected incidents to affected Unit/Departmental Managers and System Stewards.

B. Incident Response Process.

The incident response process is initiated with a suspected security breach of unencrypted electronic restricted data, as the term is defined in Section III,

Definitions, of these Implementation Guidelines. As soon as the UCSC Security Team becomes aware that a suspected security breach involves a system containing electronic restricted data (or directly involves electronic restricted data), it will notify the IT Policy Office and the Vice Chancellor, Information Technology (VC IT). Upon receipt of this notification, the VC IT will send an alert to the Campus Incident Response Team (CIRT) and file an initial report of the suspected breach to the Associate Vice President for Information Resources and Communications at UCOP.

The System Steward or designee must complete the *Initial Incident Report* (Appendix A), and submit same to the UCSC Security Team as soon as possible, but no later than 24 hours after becoming aware of the suspected breach. The UCSC Security Team and the IT Policy Office will coordinate to ensure Appendix A is completed and forwarded to the VC IT as the campus Designated Authority. The VC IT will forward the *Initial Incident Report* to the CIRT. The System Steward or designee may also file a police report with the UCSC Police Department if criminal activity is suspected.

The UCSC Security Team and Service Provider shall work together to restore the service and integrity of the system with appropriate documentation and preservation of evidence.

As soon as the UCSC Security Team has conclusively determined whether restricted data may have been acquired by an unauthorized individual, they will send a second communication to the IT Policy Office and the VC IT, informing them of the determination. If there is no possibility of unauthorized access, the VC IT will so inform the CIRT and UCOP and will forward closure reports (Appendices B/B-Alt & C) when applicable. If there is a possibility of unauthorized access, the VC IT will convene the CIRT to determine whether criteria for notification have been met.

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

Upon resolution of the breach, the UCSC Security Team and the IT Policy Office will coordinate to ensure completion of the appropriate CIRT Report (Appendix B or B-Alt) and VC IT Closure Report (Closure Report – Appendix C) and submission of the Reports to the VC IT as the campus Designated Authority as soon as possible.

The VC IT will submit a Closure Report (Appendix C) to the Associate Vice President for Information Resources and Communications at UCOP as soon as the incident is closed, or if any problem is encountered during the notification process (see below). This report will provide:

- a description of the incident, including the nature of the incident and the numbers of individuals impacted,
- the incident handling process,
- a copy of the notification, if any,

- the actions taken to prevent further breaches of security (in the event of corrective or disciplinary action, the report will not identify the affected individual(s)).

C. Notification Procedures.

If unencrypted electronic PII is reasonably believed to have been acquired by an unauthorized person, state law requires notification to subjects. The CIRT may also determine that notification is appropriate in situations involving other types of restricted data.

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
- when necessary to discover the scope of the breach and restore the integrity of the system.

The CIRT Report and the authorization from Law Enforcement initiate the notification procedures.

The VC IT works with the System Steward or designee and Service Provider to determine the availability of contact information for notification.

The VC IT along with the CIRT determines the notification plan, including the means and text of notification, consistent with IS-3 Section III.D, Incident Response Planning and Notification Procedures. Sample language is included as Appendix D, below, and on UCOP's Security Breach Notification website, <http://www.ucop.edu/irc/itsec/securitybreach.html>. The VC IT and the CIRT will determine if additional advice or assistance will be given to the affected subjects.

Upon approval of the notification plan by Campus Counsel, the VC IT works with the Public Information Office (PIO) to deliver the notification. The VC IT will work with the System Steward or designee and Service Provider as required for additional advice or assistance to affected subjects.

D. Release of Information.

Requests for information regarding a security incident from University employees without a clearly defined business need to know, or from any individuals or entities outside the University must be directed to the Operations Director in the Office of the Campus Provost/Executive Vice Chancellor. The decision to release information based on these requests will be made on a case-by-case basis, consistent with the University's obligations under the law and University policy. Information about any incident that is under police investigation will not be released until the case is closed.

Note: Written correspondence, such as email, created during the discovery or investigation phase of a security incident may be considered a public record subject to release under the California Public Records Act and/or the Information Practices Act. Therefore, information that is not appropriate for release based on the protection of privacy interests or security considerations (e.g., names of individuals or other identifying information or technical information that could enable another breach) should not be included in this correspondence. This is especially important to take into consideration where notification may be required.

VII. Responsibilities and Authority

The *UCSC Implementation Plan for Protection of Electronic Restricted Data* implements the regulations of the University of California, which prescribe compliance with existing state and federal laws. Additional authorities and specific areas of responsibility are as follows:

A. Information Technology Services

The Vice Chancellor, Information Technology, has been designated by the Chancellor to act as the lead campus authority for this Implementation Plan and has the following responsibilities under these procedures:

- Ensure that the campus incident response process is followed.
- Ensure that system-wide and campus notification procedures are followed.
- Coordinate campus procedures with Campus Counsel and other members of the Campus Incident Response Team.
- As required for breaches of unencrypted Restricted Data, provide initial and closing reports to University of California, Office of the President (UCOP).

B. System Steward

This is the individual with ultimate responsibility for a defined set of University electronic information. This person is responsible for determining the purpose, function, appropriate access to and use of, degree of sensitivity, criticality, and risk tolerance of a data set, and for communicating this information to Service Providers, Unit or Departmental Managers/Supervisors and Deans to enable appropriate implementation.

Each System Steward has the following additional responsibilities under these procedures:

- Ensure that the procedures in this document are followed for all breaches of electronic restricted data under their jurisdiction.
- Submit Initial Incident Reports to the UCSC Security Team (this responsibility may be delegated).
- Participate in notification as requested by VC IT and the Campus Incident Response Team.

C. Service Provider

Service Providers are responsible for ensuring the appropriate technical protection of restricted data on systems under their control, including any downloading of such information or temporary storage on other systems. Service Providers are also responsible for regular operational support, backup, and system maintenance of a system with electronic restricted data. Often one Service Provider has primary responsibility or oversight for a given system and may be designated the Responsible Service Provider.

Each Service Provider has the following responsibilities under these procedures:

- Ensure appropriate technical measures and checks are in place for protection of electronic restricted data under their control, including any downloading of such information.
- Ensure that the procedures in this document are followed for all breaches of electronic restricted data, or of systems containing or accessing electronic restricted data, under their management.
- Alert System Steward or designee and the UCSC Security Team of possible security breaches.
- Provide ongoing protection of electronic restricted data.
- Work with the UCSC Security Team to restore system integrity and provide information about the breach and scope.

For electronic PII, each Service Provider has the following additional responsibilities:

- Ensure that the procedures in Section V, Personal Identity Information (PII) Inventory, are followed, as appropriate to his or her title and job duties.
- Participate in notification as requested by VC IT and the Campus Incident Response Team.

D. UCSC Information Systems Security Team (UCSC Security Team)

The UCSC Information Systems Security Team has the following responsibilities under these procedures:

- Confirm that a security breach of unencrypted electronic PII or electronic restricted data has taken place.
- Resolve the security breach.
- Work with System Stewards or their designees and the members of the IT Policy Office to ensure timely, complete Initial Incident Report, CIRT Report, and Closure Report (Appendices A, B/B-Alt, and C)
- Notify the IT Policy Office and the VC IT as soon as Team members become-aware that a suspected security breach involves a system containing electronic restricted data (or directly involves electronic restricted data), and again when a determination is made as to whether this data may have been accessed without authorization.

E. ITS Support Center

Escalate reports of potential security breaches involving restricted data to the UCSC Security Team.

F. IT Policy Office

Work with UCSC Security Team to facilitate timely completion and submission of Initial Incident Report, CIRT Report, and Closure Report (Appendices A, B/B-Alt, and C) to VC IT.

G. Campus Incident Response Team (CIRT)

Campus units have responsibilities within these procedures as members of the Campus Incident Response Team (CIRT). In partnership with the VC IT and as required, the System Steward and/or Service Provider, they ensure the consistency of response and when required the completion of notification procedures.

VC IT as member of the CIRT:

- Determine that the criteria for notification have been met.
- Develop notification plan.
- Perform notification and respond to inquiries from affected subjects.

UCSC 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.

Campus Counsel:

- 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.

Internal Audit:

- Validate and/or substantiate the methods and conclusions for determining if criteria for notification have been met; provide related advice as appropriate.
- Advise and review means and text of notification.

Campus Provost/Executive Vice Chancellor (CP/EVC):

- Advise if criteria for notification have been met.
- Identify if breach resulted in violations of additional elements of the California Information Practices Act or other laws or regulations governing the management of information.

H. Human Resources – Staff or Academic, as appropriate

Advise in the event that personnel or disciplinary action is deemed necessary in response to a security breach or violation.

VIII. Contact Information and Getting Help

Contact Information for Security Breach Procedures:

Internal Audit	(831) 459-3205, internal.audit@ucsc.edu
IT Policy Office	itpolicy@ucsc.edu
ITS Divisional Liaisons	http://its.ucsc.edu/divisional_liaisons/index.php
ITS Support Center	(831) 459-HELP, help@ucsc.edu , http://its.ucsc.edu/support_center/ , or M-F 8AM - 5PM, 54 Kerr Hall
ITS Service Manager for Community and Compliance	itpolicy@ucsc.edu , (831) 459-2779
UCSC Information Systems Security Team (UCSC Security Team)	security@ucsc.edu Reporting security incidents online: http://its.ucsc.edu/security/report.php
UCSC Police Department	(831) 459-2231, http://www2.ucsc.edu/police/

Getting Help:

For help with...	Contact...
...technical or other questions about this Implementation Plan and related procedures ...training and assistance to campus units on topics associated with systems security and appropriate systems controls	The ITS Support Center or your ITS Divisional Liaison
...compliance controls and procedures	Internal Audit

IX. Related Policies / References for More Information

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/oip/privstat.htm>

[US] Department of Health and Human Services, Office of the Secretary, 45 CFR Parts 160, 162, and 164, Health Insurance Reform: Security Standards; Final Rule (The

HIPAA Security Rule):

<http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf>

State of California Statutes

State of California Information Practices Act of 1977 (Civil Code Section 1798 et seq.)

<http://www.privacy.ca.gov/code/ipa.htm>

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

<http://www.privacyprotection.ca.gov/code/pr.htm>

University of California

University of California Policies

<http://www.ucop.edu/ucophome/coordrev/ucpolicies/>

University of California Business and Finance Bulletins

<http://www.ucop.edu/ucophome/policies/bfb/>

Information Resources & Communications Security Breach Notification website

<http://www.ucop.edu/irc/itsec/securitybreach.html>

University of California, Santa Cruz

UCSC – Official Policies and Procedures

<http://www.ucsc.edu/ppmanual/>

UCSC Staff Procedure for responding to Public Records Requests or other Requests for Information

<http://iam.ucsc.edu/respondrecordsrequests.html>

Announcement of UCSC Guidelines and Implementation Procedures for management of computerized identity information from Larry Merkley, Vice Provost, Information Technology, to Principal Officer, Department Chairs and Unit Heads, May 1, 2003

[Document temporarily offline]

Protecting Electronic Restricted Data:

- *UCSC Practices for Protecting Electronic Restricted Data:*
<http://its.ucsc.edu/security/policies/rd.php>
- *Restricted Data Resources:*
http://its.ucsc.edu/security_awareness/restricted_data_resources.php

PII Resources:

- *ITS' Personal Identity Information Resources web page:*
http://its.ucsc.edu/security_awareness/pii.php
- *Online Computer Security Awareness Training, Including Protecting PII and Other Restricted Data:*
http://its.ucsc.edu/security_awareness/training.php

UCSC's University Administrative Information Systems Access to Information Statement
http://its.ucsc.edu/services/accounts/online_forms/acc_info_stmt.pdf

UCSC Office of the Registrar FERPA Information:

- *UCSC Administrative Procedures Applying to Disclosure of Information from Student Records:*
<http://reg.ucsc.edu/guidelines.html>
- *UCSC Policy on Privacy of Student Records – A Quick Reference:*
http://reg.ucsc.edu/disclosure_qr.pdf

Industry Partners

Payment Card Industry (PCI) Data Security Standard
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

X. Appendices

- Appendix A:** Initial Incident Report
- Appendix B:** Campus Incident Response Team (CIRT) Report
- Appendix B-Alt:** Alternate CIRT Report
- Appendix C:** VC IT Closure Report to UCOP
- Appendix D:** Sample Notification Text
- Appendix E:** Visual Breach of Security Procedures

**Appendix A:
Initial Incident Report**

To be submitted by the System Steward or designee to security@ucsc.edu, itpolicy@ucsc.edu, and the Vice Chancellor, Information Technology as soon as possible, but no later than 24 hours after breach is *suspected*.

<i>Potential scope of breach</i>	
<i>Source of breach</i>	
<i>General description of data compromised</i>	
<i>Potential population</i>	
<i>Controls in place or other historical information</i>	
<i>Time <u>estimate</u> to resolve breach</i>	

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

**Appendix B:
Campus Incident Response Team (CIRT) Report**

*To be used for suspected or confirmed breaches of PII, ePHI, PCI, and FERPA-protected data,
or of systems containing or accessing these types of data
(See Appendix B-Alt for other types of breaches.)*

To be submitted by UCSC Security Team or the IT Policy Office to Vice Chancellor,
Information Technology as soon as possible after breach is **resolved**.

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

FACTORS to CONSIDER for NOTIFICATION

- 1. Indications that the information is in the physical possession and control of an unauthorized person....*
- 2. Indications that the information has been downloaded or copied....*
- 3. Indications that the information was used by an unauthorized person....*
- 4. Duration of exposure*
- 5. The number of individuals affected*
- 6. The number of different types of information that may have been acquired*
- 7. The extent to which the compromise indicates a directed attack*
- 8. Indication that the attack intended to seek and collect personal information*

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

HISTORY and/or TECHNICAL DETAILS
Provide if available and relevant

**Appendix B-Alt:
Alternate CIRT Report**

To be used for breaches of systems that are determined not to contain or access PII, ePHI, PCI, or FERPA-protected data.

(See Appendix C for breaches involving PII, ePHI, PCI, or FERPA-protected data.)

To be developed by the members of the IT Policy Office in conjunction with System Steward or designee and UCSC Security Team as soon as possible after breach is **resolved or is determined not to involve PII, ePHI, PCI, or FERPA-protected data.**

Relates to:

- Electronic Protected Identity Information (PII)*
- Electronic Protected Health Information (ePHI)*
- Payment Card Information (PCI)*
- Confidential Student Record Data (FERPA-protected Data)*
- Other Restricted Data*

SUMMARY

Provide a summary of the outcome of the data breach. Include any or all of the following information, as relevant. Expected length: approx 1/2 page.

- How the breach was discovered*
- Scope of breach*
- Source of breach*
- Description of data compromised*
- Affected population*
- Actions taken to prevent further breaches of security*
- Time to resolve breach*

Note: For breaches that were initially thought to involve PII, ePHI, or PCI that are determined not to involve these types of data, conclude with the following sentence:

The threshold for launching the campus incident response process was not met, as there was no suspected security breach of PII, ePHI, or PCI.

Note: For suspected and confirmed breaches of FERPA-protected data, conclude with the following sentence, and forward a copy of this completed summary report to UCSC Registrar:

This incident report is being shared with the Registrar's office for handling with regard to FERPA.

HISTORY and/or TECHNICAL DETAILS

Provide if available and relevant

Appendix D: Sample Notification Text

Universitywide requirements for notification of individuals when their personal identity information (PII) has been acquired by an unauthorized individual through a security breach are found in Business and Finance Bulletin, IS-3, Section III.D, Incident Response Planning and Notification Procedures.

The following text is intended to provide guidance in developing a notice to subjects of a database compromise. Sample language is also available on UCOP's Security Breach Notification website, <http://www.ucop.edu/irc/itsec/securitybreach.html>. The final text that is used in any actual breach notification should be reviewed by Campus 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]*

Appendix E: Visual Breach of Security Procedures

