



University of California

UCOP Guidelines for Protection of Electronic Personal Information Data and for Security Breach Notification

UCOP Implementation Plan for Compliance with Business and Finance Bulletin IS-3, Section III.D.2, "Notification in Instances of Security Breaches Involving Personal Information Data"

Information Resources and Communications

May 30, 2003

Revised December 15, 2008

Table of Contents

I. UCOP Implementation Plan	3
A. Definitions.....	3
B. Personal Information: Protection and Notification Requirements	5
C. Database Management Procedures.....	6
D. Procedures for Response to a Breach of Security	8
II. Summary	12
A. Data Protection and Notification Planning Phase	12
B. Breach of Security Response Phase	12

I. UCOP Implementation Plan

Universitywide procedures for notification of individuals in the case of security breaches as well as the requirement for the establishment of local (campus) implementation plans are published in Business and Finance Bulletin IS-3, “Electronic Information Security,” section III.D.¹ In accordance with the Universitywide procedures, the Associate Vice President for Information Resources and Communications (AVP–IR&C) has been designated the lead UCOP authority for ensuring compliance with the notification requirements and the local UCOP implementation plan, “UCOP Guidelines for Protection of Electronic Personal Information Data and for Security Breach Notification.”

The UCOP implementation plan defines requirements for management of all computerized information that could be used to impersonate an individual in ways that might cause serious loss of privacy and/or financial damage. In essence, departments with functional responsibilities that require collection or management of personal information must protect such data appropriately and also must notify individuals whose personal information has been acquired through a breach of security. These guidelines apply only to electronic, not hard copy, forms of such information² and augment the security requirements defined in IS-3.

A. Definitions

Certain terms used within these guidelines are defined as follows.

1. Database

A database is any collection of information on computer media that contains information about individuals in an organized form such that information about a particular individual may be distinguished from information about other individuals. This includes large databases such as DB2, Sybase, or Oracle; departmental database systems such as Microsoft SQL Server and MySQL; and simple text files, spreadsheets, etc. Examples of databases that might fall under these guidelines include

- Corporate personnel databases
- Credit card sales records
- Personal travel profiles
- Departmental personnel office employee records
- Student loan records
- Risk Management claims records

¹ See <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>.

² Paper records must be managed as required under the Records Management and Privacy series of Business and Finance Bulletins.

This definition is not dependent on where the database is stored. Databases may exist on hard drives, magnetic tape, optical disks, diskettes, personal digital assistants (PDAs), etc.

2. Functional Roles

Each department head is responsible for ensuring that these guidelines are followed for all databases managed within the department. IS-3 defines several functional roles with respect to electronic information resources.³ The department head must determine how these roles are fulfilled.

A distinction is made between the department that has responsibility for the existence of a particular database and, if different, the department or unit that has responsibility for operational support. The department that created or was given responsibility for the existence of the database as part of its business function is the “proprietor” of the database and therefore has responsibility for its security and management, including the required notification procedures.

a) Database Proprietor

The department head may delegate the role of “database proprietor” to a manager within the same department. A database proprietor is an “electronic information resource proprietor” as described in IS-3. The database proprietor is given specific responsibilities in these guidelines with respect to security of the database and must ensure that notification to database subjects of security breaches is completed.

b) Database Custodian

The department head or database proprietor may delegate physical management of the database to a “database custodian.” A database custodian is an “electronic information resource custodian,” as described in IS-3. The database custodian typically will be the first to notice an anomaly or security breach and may be in the best position to take steps to mitigate any further losses with respect to the database or the database platform. The database custodian must alert the database proprietor of reasonably suspected security breaches.

3. Personal Information

Personal information is data that pertains to a given individual, for example, name, address, telephone number, etc. These guidelines apply specifically to databases containing personal information as defined in section I.B.

4. Restricted Database

A database that includes personal information is a “restricted” database, as defined in IS-2, “Inventory, Classifications, and Release of University Electronic Information”.⁴ Access to such a database must be managed appropriately and, in the case of a breach of

³ See IS-3, Appendix A, “Definitions”

⁴ See IS-2, Appendix A, “Definitions”

security that is reasonably believed to have led to a compromise of the personal information it contains, notification to affected database subjects is required.

5. Security Breach

A security breach occurs when an individual's unencrypted personal information is reasonably believed to have been acquired by an unauthorized person. Good faith acquisition of personal information by a University employee or agent for University purposes does not constitute a security breach, provided that the personal information is not used or subject to further unauthorized disclosure. If personal information in the database is encrypted, a breach occurs only if an access method was used, or is reasonably believed to have been used, that resulted in decryption; or if data was compromised on a desktop or other platform that had acquired a clear text copy of that data.

B. Personal Information: Protection and Notification Requirements

1. Data Elements to Be Protected

Any database containing records that include *any two or more* of the following personal information elements pertaining to the subject of that record constitutes a restricted database and *must be managed and protected* according to the guidelines in this document. UCOP has identified a list of data elements (a–g below) for protection that extends the list covered by legal notification requirements, which are described in section I.B.2. The purpose of broadening the list is to provide some protection against correlation of data across two or more databases.

- a) Subject's first name or initial, and last name
- b) Social Security number
- c) Driver's license number or state-issued identification card number
- d) Account number,⁵ 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
- e) Date of birth
- f) Passport number
- g) Health insurance information
- h) Personal health information

2. Legal Notification Requirements

California law *requires* notification to database subjects who are California residents when, through a security breach, as defined, unencrypted copies of item (a) plus at least

⁵ "Account number" corresponds to an individual's financial account.

one of items (b), (c), (d), (g), or (h) are reasonably believed to have been acquired by an unauthorized person.⁶ In addition, many other states – and countries - also require notification in various breach circumstances. In general, where notification has been determined to be appropriate, it should be given to all affected persons irrespective of their place of residence.

3. UCOP Notification Policy

Database proprietors must meet the legal requirements for notification. In addition, notification of database subjects should be *considered*, in coordination with the Office of General Counsel, when any two of the broad list (a–h) of computerized data elements, when unencrypted, are reasonably believed to have been acquired by an unauthorized individual.

C. Database Management Procedures

The following procedures are required of any department that is responsible for a restricted database, irrespective of whether the contents of the database are encrypted.

Please note that personal information may exist temporarily outside of its original database. Although the original database record might be encrypted, the data may exist occasionally in unencrypted form which, if compromised, could result in a required notification.

1. Internal Departmental Database Inventory

All UCOP departments that have primary responsibility for the existence of a restricted database should maintain an internal inventory of all such databases within the department's control. By June 30 of each year, the department head must provide the AVP–IR&C with an up-to-date list of the databases in this inventory. Any significant new databases, or any database enhancements that result in an existing database falling under these guidelines, may be added to the list and reported to the AVP–IR&C at any time. A form that may be used for the database list is posted on the IR&C Web site.⁷

The internal inventory requirement does not apply to temporary downloads of database information to a personal computer for the purpose of processing or analyzing the information, provided the download does not reside on such a computer for more than a few days. However, the person downloading that data becomes a temporary database custodian; the database proprietor continues to assume full responsibility for the protection of that data and notification to subjects in the event of a security breach.

E-mail that contains personal information may not in itself constitute a database for purposes of the database inventory. However, if there is a security breach involving e-mail that contains personal information, the incident should be reported to the AVP–IR&C and notification to the subject(s) should be undertaken at the discretion of the department head.

⁶ See California Civil Code Section 1798.29.

⁷ See <http://www.ucop.edu/irc/itsec/welcome.html>.

The database list to be reported to the AVP–IR&C must include the

- Name of the department,
- Names of the database proprietor and the database custodian, and
- Title of the database

When conducting their internal inventory of databases, departments may find it helpful to collect the following information as a means to assess current security measures and to prepare for meeting the incident response and notification requirements.

- A list of the personal information elements that are included in the database and a notation whether or not they are stored in encrypted form
- The physical location of the platform(s) holding the data
- A brief description of the intended users and uses
- A brief description of available access methods, such as direct login, on-line downloading, and/or database query
- A brief description of logical security controls, for example, UserID and password, and whether downloads are allowed, and how access is logged
- For each discrete physical location housing database platforms, a brief description of the physical access controls in effect at that location, e.g., electronic security lock, entry log, or the equivalent

This additional information is not to be reported to the AVP–IR&C. If collected, this additional information must be guarded carefully as it could be used to gain unauthorized access to the databases it identifies.

2. Subject Contact Information

All database proprietors should have contact information, to the extent possible, for each relevant database subject, including the subject's e-mail address and primary U.S. postal address. Contact information does not need to be stored in the same restricted database; it could be stored in a parallel database for this specific purpose. Contact information should be kept valid and up-to-date if it is feasible to do so.

3. Database Protection

Database proprietors must ensure that appropriate measures and checks are in place for the protection of personal information databases. It is strongly suggested that all personal information be encrypted while in storage in order to avoid possible compromise of that data and subsequent requirements for notification of subjects. If there is any question about the adequacy of current controls, a review by IR&C and UCOP Internal Audit should be requested.

Database proprietors must inform all staff members who make use of the database of the legal and institutional requirements for protection of personal information. Such information should be shared only with those who need the data to perform their assigned duties. Such information should never be left exposed on a computer screen if the

responsible staff member is absent. E-mail that contains personal information must be treated with care and should not be preserved any longer than necessary.

If a business process requires that database records be shared with another campus or a contractor, that party should be informed of these protection and notification requirements as part of their role as proprietor of the information they receive. In the case of a security breach, the University department that originated the database should be involved directly in incident analysis and notification activities.

All access to the database platform must be logged. All access to the database itself also should be logged if possible. This logging requirement does not apply to personal computers or PDAs. However, downloads of personal information to personal computers or PDAs should be logged at the source so that there is a record of what information was copied, to where, when, and by whom. This will allow notification in case the personal computer or PDA is lost or compromised.

Log files should be reviewed daily by database custodians, possibly with the aid of automated tools, and at least monthly by database proprietors.⁸

Database platforms and systems, especially those with connection to the Local Area Network, should be maintained with all relevant security updates and patches, as defined in IS-3.

Database backup and business continuity procedures must be adequate to protect personal information. If backup copies are taken off-site and the individual personal information elements are not encrypted, then the entire database should be encrypted.⁹

D. Procedures for Response to a Breach of Security

1. Security Breach Suspected or Detected

a) Alert the database proprietor as soon as a breach is suspected to have occurred, or system monitoring or log files indicate anomalous activity.

The database custodian must immediately alert the database proprietor whenever a security breach is suspected or system monitoring or log files indicate anomalous activity.

b) Secure the system or take it temporarily off-line.

The first priority is to prevent further intrusion to the system or exposure of personal information. The database custodian must secure the system or take the affected server(s) off-line until that type of breach can be prevented from recurring. If there is reasonable doubt about whether the method used to breach security has been eliminated, the system must be taken off-line. If it is suspected that any system configuration or software has been modified by the perpetrator, a complete system integrity check should be initiated. This action must proceed independently of the notification process.

⁸ See IS-3.

⁹ See IS-3, Section III.C.2.c.ii, "Backup and Retention."

c) Collect information supporting the observation of a real or suspected breach.

The database custodian must collect all information that relates to a possible security breach and store it safely, preferably off-line. It is critical that log files and all other records pertaining to the security breach be preserved in a manner that prevents their being modified or lost. These data may also be requested by law enforcement. All such records must be retained for a minimum of three years, or if there is any pending litigation involving the particular breach, until the litigation is finally concluded, whichever is longer.

d) Report the breach in writing immediately (in no more than twenty-four hours) to the AVP-IR&C, who convenes the incident response team.

Any known or reasonably suspected breach of security of any restricted database must be reported to the AVP-IR&C immediately in writing no more than twenty-four hours after its discovery. The AVP-IR&C will activate a Security Incident Response Team consisting of the department head, a subject matter expert from the department, the UCOP Information Security Officer, the IT Policy Director, the SVP-Compliance and Audit (or designee), a representative from General Counsel, UCOP Strategic Communications, and UCOP Internal Audit. The incident response team also will notify the appropriate law enforcement office as necessary.

2. Incident Review

a) Conduct an incident review; determine whether notification is required.

The database proprietor, together with the incident response team, must assess the likelihood and potential scope of any security breach. Elements of this assessment shall include the number of subjects affected and which data elements were likely to have been compromised.

Notification is required by state law, as described in section I.B of this plan. The criteria for notification should include the likelihood of a compromise having occurred, the data elements potentially compromised, and the potential consequences from such compromise to the individual as well as to the University. If there is any doubt about the need for notification, the database proprietor or department head should consult the AVP-IR&C and the Office of General Counsel.

b) If notification is required, the department is responsible for conducting it.

The department is responsible for conducting all aspects of the notification, with guidance from the Security Incident Response Team, and following the requirements in “Breach of Security Notification” (see section I.D.3).

3. Breach of Security Notification

When notification to affected database subjects is required, it shall be made in the most expedient manner possible and without unreasonable delay, consistent with the legitimate needs of any measures necessary to determine the scope of the breach and restore the reasonable integrity of the database platform or system. If law enforcement is involved in the investigation of a breach, the required notification should be delayed until the law

enforcement agency determines that such notification no longer will impede or compromise its criminal investigation.

The notification text should explain the nature of the suspected compromise of information and suggest where the subject might turn to find information about mitigating or minimizing identity theft. The draft notification text should be reviewed by the Security Incident Response Team before being issued. Sample notification text is presented on the IR&C Web site.¹⁰

Individual direct notification should be undertaken whenever possible. If the list of individual database subjects reasonably thought to have been affected by a security breach is not known, all database subjects must be notified. Notification to affected database subjects may take the form of e-mail or of written, hard copy. E-mail may be preferable as long as reliable e-mail addresses are maintained for the affected individuals. Campus or U.S. postal mail must be used if a suitable e-mail address is not available. If an e-mail results in a returned error message, written notification should be performed.

Substitute notice may be used only when contact information is not available. Substitute notice should include prominent notification on the department's customer Web site or other commonly used Web location, along with any additional notification mechanisms that may be considered appropriate by the Security Incident Response Team. Web site notice shall remain in place for at least forty-five days. An audit trail of what notification was issued, including date/time, method, text of notification and, if applicable, the list of individuals notified, must be maintained.

4. Credit Monitoring Services

Under certain circumstances, credit monitoring services may be offered to individuals who are notified that their personal information was involved in a security breach.

Credit monitoring services provide a variety of options for a fee. However, some credit protection services, namely credit reports and credit fraud alerts, are available free of charge to all individuals directly from the three credit bureaus (Equifax, Experion, TransUnion). Most credit card companies and other creditors will not issue credit without first checking the applicant's credit history. A fraud alert tells credit issuers that there is possible fraud associated with the account and gives them a phone number to call before issuing new credit in your name. This is intended to prevent others from fraudulently receiving credit in an individual's name. Placing a fraud alert with any one of the three credit bureaus will trigger a process by which the individual will be instructed on how to obtain a free credit report (which the individual must request). An initial fraud alert lasts ninety days and may be reinstated every ninety days.

The decision whether to offer credit monitoring services should be made before the notifications are issued so that, if applicable, the offer can be communicated as part of the notification. The EVP-Business Operations, in consultation with the department head, AVP-IR&C, SVP-Compliance and Audit, and the General Counsel, is responsible for the decision.

¹⁰ See <http://www.ucop.edu/irc/itsec/securityimplementation.html>

The following criteria must be met before an offer of credit monitoring services may be considered:

1. The incident involves a clearly identifiable breach of personal information requiring notification of affected individuals, as required in California Civil Code 1798.29.

and

2. Personal information that could lead to credit fraud was exposed as a result of the breach. These are items (a) plus (b) or (d) as described in section I.B.1.¹¹

and at least one of the following:

- a. There is clear evidence of misuse of one or more individuals' personal information.
- b. There is clear evidence that the incident was malicious and that personal information was the target.
- c. Any of the personal information involved in the breach belongs to a third-party that either is operating under a legal obligation (e.g., court order) to provide credit monitoring services or has a documented policy of offering credit monitoring services in the event of a breach.

5. Incident Closure Report

A closure report must be submitted to the AVP-IR&C and the SVP-Compliance and Audit as soon as the subject notification process is completed, or if any problem is encountered to significantly delay that process. This report should detail the nature and cause of the incident, what type of notification was used and to whom it was sent, the response process, and what steps have been taken to prevent a recurrence of such an incident.

¹¹ California Civil Code 1798.29 requires notification to individuals when specific information is obtained or reasonably believed to have been obtained by an unauthorized individual – however, some of the information cited in California Civil Code 1798.29, such as personal health information, cannot be used for credit fraud.

II. Summary

The UCOP implementation plan describes basic steps for protecting and managing personal information and for responding to a security breach. These steps are summarized below. Please refer to the full implementation plan for greater detail and explanation.

A. Data Protection and Notification Planning Phase

1. Conduct an internal departmental inventory of databases containing personal information.
2. Submit a list of the department's databases annually (June 30) to the AVP-IR&C. Provide the
 - Name of the department,
 - Names of the database proprietor and the database custodian, and
 - Title of the database.
3. Review and update contact information as possible.
4. Ensure appropriate measures are in place to protect databases with personal information.
 - If desired, request a review of security measures by IR&C and Internal Audit.
 - Inform all staff members who work with personal information databases about security guidelines.
 - Log all access to database platforms, and to the database itself, if possible.
 - Log downloads of personal information to personal computers or PDAs at the source.
 - Ensure daily review of log files by database custodians.
 - Ensure monthly review of log files by database proprietors.
 - Maintain database platforms and systems with relevant security updates and patches.
 - Review backup and business continuity procedures; ensure that entire backup databases are encrypted, or just the personal information elements in the backup database.

B. Breach of Security Response Phase

1. Alert the database proprietor as soon as a breach is suspected to have occurred, or system monitoring or log files indicate anomalous activity.
2. Secure the system or take it temporarily off-line.
3. Collect information supporting the observation of a real or suspected breach.

4. Report the breach in writing immediately (in no more than twenty-four hours) to the AVP-IR&C, who convenes the Security Incident Response Team.
5. Conduct an incident review; determine whether notification is required.
6. If notification is required, the department is responsible for conducting all aspects of the notification, with guidance from the Security Incident Response Team.
7. Conduct direct notification by
 - e-mail or
 - written, hard copy; or,
 - if sufficient contact information is not available for e-mail or hard copy notice, place a notice on a commonly used Web site for at least forty-five days.
8. Submit a closure report to the AVP-IR&C and the SVP-Compliance and Audit that describes the
 - Nature and cause of the incident,
 - Notification process,
 - Response process, and
 - Steps taken to prevent recurrence of the incident.