UC Davis Campus Incident Response/Notification Guidelines
For Unauthorized Acquisition of Protected Data

Background

Identity theft is a serious crime. In the United States, an estimated 160,000 persons fell victim to identity theft in 2002, sometimes with devastating consequences. When an individual's identity has been stolen, the victim could be forced to spend months or years to clear up his/her credit record. Moreover, victims could be refused bank loans or arrested for crimes they did not commit. The pervasiveness of computer systems hosting personal information (such as name, Social Security numbers, date of birth, driver's license number, credit card numbers, ATM card numbers, telephone calling cards) and computer system security vulnerabilities have resulted in the passage of new consumer protection laws. In 2002, a new law was passed in California requiring organizations to notify state residents when a computer security breach has permitted the release of personal information to unauthorized recipients.

This new law, amending section 1798 of the California Civil Code, will influence operational practices at UC Davis. The University of California has recently adopted an Information Security policy (BFB IS-3) revision to implement the provisions of this new law. The new law and policy take effect on July 1, 2003.

In early June, Chancellor Vanderhoef requested the campus Information Technology Security Coordinator to take the lead in developing an implementation plan of this new law. The Chancellor also communicated the significance of this new law to the Deans, Vice-Chancellors and Vice Provosts. This communication underscored the need to reduce the number of computing systems hosting personal information and to secure the remaining systems that must store personal information. This document describes the UC Davis implementation plan for responding to the new law and UC policy.

Summary of Implementation Guidelines (Attachment A)

Wherever possible, it is recommended that campus units avoid establishing new computer systems hosting personal information and reduce the number of existing computer systems that provide access to personal information. For those computer systems with personal information that must remain in operation, the campus unit responsible for these systems must:

- have knowledge of the purpose, location and responsible parties for the computer systems,
- physically and administratively secure the computer systems,
- monitor the use of the computing systems,
- immediately remove compromised systems from the campus network for inspection and remediation

- immediately notify their respective Dean, Vice-Chancellor, Vice-Provost or other senior campus administrator should a security breach in a computer system under their management result in the unauthorized acquisition of personal information

The Deans, Vice-Chancellors and Vice-Provosts are responsible under this new law to:

- report security breaches within computing systems hosting personal information to Robert Ono, the campus IT Security Coordinator.
- if authorized by the Chancellor or Provost/Executive Vice Chancellor, notify individual record owners about the unauthorized acquisition of personal information.

Any incident that results in unauthorized acquisition of personal information from a computer system will be summarized and reported to the University of California Office of the President by the campus IT Security Coordinator.

The attached documents further elaborate on the implementation guidelines. For assistance or questions regarding the guidelines, please contact the campus IT Security Coordinator, Robert Ono (530-754-6484 or raono@ucdavis.edu).

Attachment A: UC Davis Implementation Guidelines

1. **Campus Guideline**: Personal information hosted on computing systems will be protected from unauthorized acquisition. Should a computer security breach result in unauthorized acquisition of personal information, information owners will be notified of the incident in a timely manner.

2. **Definitions**
   2.1. **Protected data**: The data comprising personal information governed by these guidelines is defined as unencrypted protected data. This protected data includes an individual's first and last name in combination with any of
   - social security number,
   - driver's license number,
   - financial account or credit card number in combination with any password that would permit access to the individual's financial account.

   2.2. **Computing system**: A computing system is any electronic programmable machine that performs high-speed mathematical or logical operations or that assembles, stores, correlates, or otherwise processes information. A computing system includes server, desktop, laptop, tablet computer, or personal digital assistant (PDA) that contains or provides network access to protected data.

   2.3. **Data proprietor**: A data proprietor is a Dean, Vice Chancellor, Vice Provost, or senior administrator appointed by the Chancellor or Provost/Executive Vice Chancellor who has been delegated the responsibility for oversight of data and/or computing systems within their organizational area. This responsibility may be further delegated within the organizational area.

   2.4. **Campus unit:** A campus unit, under the general direction of the data proprietor, is responsible for the implementation of logical and physical control over data systems and the technical management of data resources.

   2.5. **Control records**: a database, spreadsheet, or any other electronic file that contains a list of computing systems that contain protected data. Control records must contain the following:
   - name of individual(s) responsible for the computing system,
   - physical location of computing system,
   - description of logical access and security controls.

3. **Responsibilities**
   3.1. **Lead Campus Security Authority:** The UC Davis Information Technology Security Coordinator is designated as the lead campus authority who is responsible for:
   - ensuring that the campus incident response process for computing systems and data resources is followed,

- ensuring that systemwide and campus notification procedures are followed,
- reviewing incidents potentially involving unauthorized release of protected data with the campus Investigations Coordination Workgroup.

3.2. **Data Proprietors** have oversight responsibility to ensure the campus units within their organization:

- develop and maintain adequate security plans for computing systems within their jurisdiction commensurate with risks associated with the sensitivity or confidentiality of data and to reduce risk of threats to protected data in computing systems within their jurisdiction,
- develop and maintain adequate procedures for granting and monitoring access to protected data,
- develop and maintain an inventory of computing systems containing protected data or have access to protected data that are subject to the requirements in these guidelines (such an inventory could be maintained in a computer database),
- collect and maintain control records for those systems determined to be subject to the requirements in these guidelines,
- should a security breach occur, ensure initial incident investigation and reporting is conducted on a timely basis.
- establish an immediate notification plan, including draft communication text, which could be implemented in the event of a breach that would have immediate deleterious impact on individuals whose personal information may have been obtained by a non-authorized source.

3.3. **Campus Units** must:

- inform users of protected data of their responsibilities to secure such data from unauthorized release,
- develop and maintain control records in a secure environment,
- evaluate risks and implement appropriate security safeguards for computing systems containing protected data within their jurisdiction,
- implement, as appropriate, encryption strategies for both the transmission and storage of protected data,
- establish monitoring procedures to identify unauthorized access to or anomalous activity occurs on computing systems. Campus Units may consult the lead campus security authority for assistance in determining security strategies appropriate to their technological environment,
- report suspected unauthorized acquisition of protected data to the data proprietor and lead campus security authority.

3.4. **Data Users** must:

- abide by established procedures on access to and use of protected data,
- protect the resources under their control, such as access passwords, computers, and data they download,

- report any unauthorized or anomalous activity to the data proprietor which may have resulted in the release of protected data to unauthorized individuals.

3.5. **Campus Investigations Coordination Workgroup**

- coordinates a review of any security breach that potentially involves the unauthorized access of protected data. The Workgroup will treat these breaches as suspected misuse of University resources,
- considers, based on findings of fact by the lead campus security authority, whether a a security breach resulted in the release of protected data to unauthorized individuals,
- recommends action by the Chancellor or Provost/Executive Vice Chancellor, based on its deliberations and findings of fact reported by the lead campus security authority, including notification by data proprietors of individuals whose personal information is reasonably believed to have been acquired by an unauthorized person,
- monitors the progress of data proprietors and campus units in respect to notification and remedial action authorized by the Chancellor or Provost/Executive Vice Chancellor, and formally closes the campus review of an incident after all required remedial actions have been taken.

4. **Incident Response Process (See Figure A)**

4.1. If a breach is suspected within a computing system that contains or has network access to unencrypted protected data, the campus unit must immediately:

- remove the computing system from the campus network,
- conduct a local analysis of the breach to identify incident cause, personal information at risk of acquisition, collect evidence of data acquisition and identify the required remedial action,
- notify the data proprietor and lead campus security authority

4.2. The lead campus security authority will review the evidence of a breach with the campus unit and make findings as to the possibility that protected data was acquired**.** If required, the lead campus security authority will arrange for additional assistance to be provided to the campus unit to preserve incident evidence and/or examine the subject computer(s).

4.3. The lead campus security authority will document its findings in a written report to the campus Investigations Coordination Workgroup, along with recommendations to management of the campus unit for addressing the causes of the security breach.

4.4. The lead campus security authority will provide its report and expeditiously notify the Workgroup if there is a reasonable belief, based on findings of fact, that unencrypted protected data has been acquired by an unauthorized source. The Investigations Coordination Workgroup will be informed of the nature of the security breach, the number of individuals affected and the remedial steps that have been taken to address the cause of the security breach.

4.5. The campus Investigations Coordination Workgroup will consider, based on findings of fact by the lead campus security authority, whether criteria for notification under California Civil Code 1798.29, 1798.82 have been met and, if they are met, consider what means of notification, e. g., email, postal mail, or website notice, should be employed. During the analysis of whether the incident supports a notification recommendation, the Investigations Coordination Workgroup will consider, among other facts, the duration of information exposure, availability of log records that provide evidence of information download or copy activity, indication that the information was actually used by an unauthorized person, indication that the information is in the physical possession of an unauthorized individual, the amount of information at risk, the extent to which knowledge about the identified computer compromise indicates the attack was part of a broad Internet exploit and whether the attack intended to seek and collect personal information, and other criteria defined by the University of California Office of the President or regulatory agencies. During the incident review, representatives of the Investigations Coordination Workgroup may meet with the Data Proprietor, or designee, as necessary, to review the incident details and notification criteria.

The Investigations Coordination Workgroup will forward a recommendation to the Chancellor or Provost/Executive Vice Chancellor concerning notification of individuals whose protected information may have been acquired by an unauthorized party.

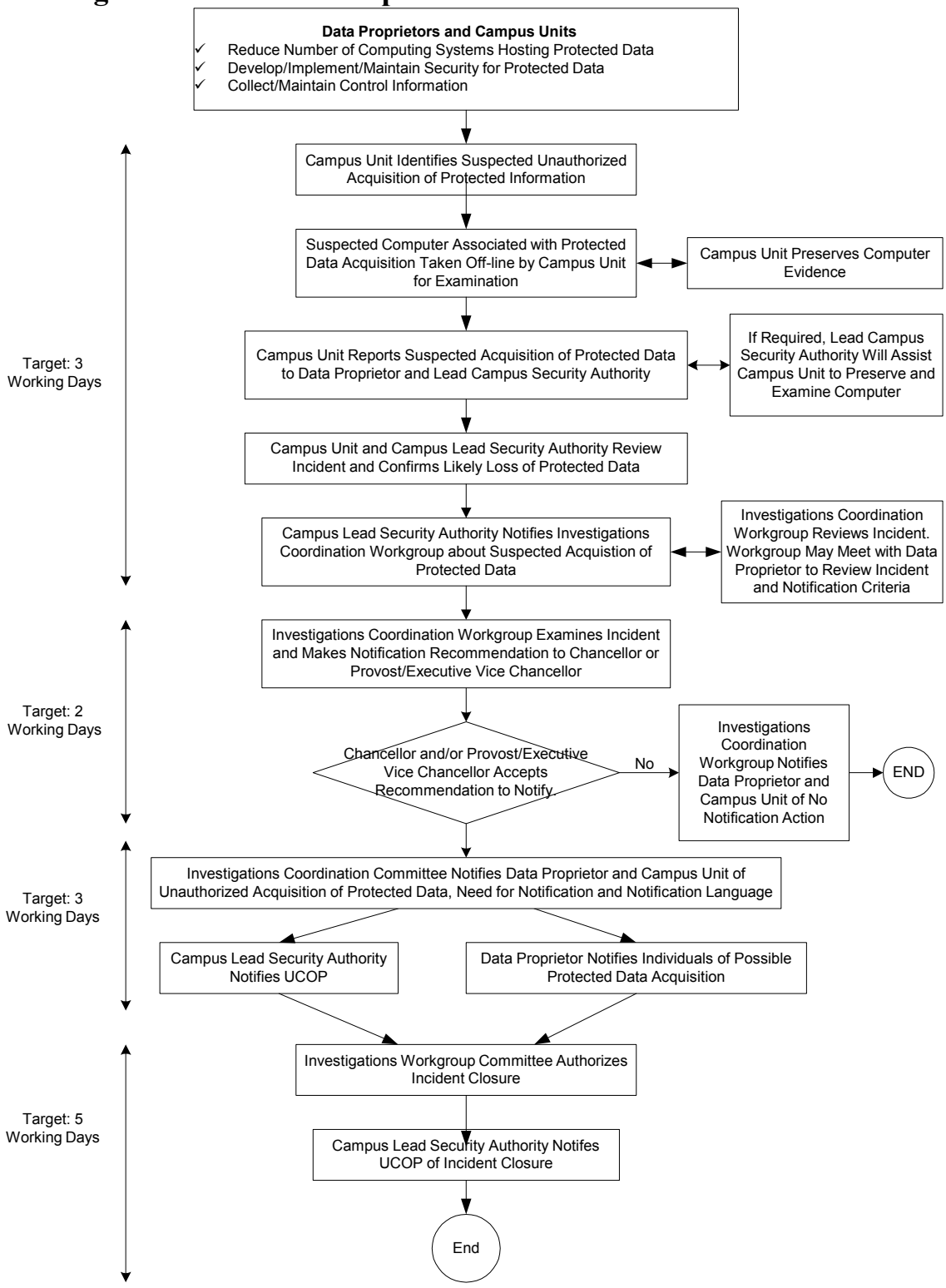
4.6. If the Chancellor or Provost/Executive Vice Chancellor determines that notification is required, the data proprietor must notify individuals of the possible information release without unnecessary delay. The lead campus security authority will immediately report the breach to the Associate Vice President for Information Resources and Communications at UCOP.

4.7. Upon closure of the incident by the Investigations Coordination Workgroup, the lead campus security authority will notify the Associate Vice President for Information Resources and Communications at UCOP of the incident closure.

5. **Local Notification Procedures**
The data proprietor will determine whatever additional advice or assistance will be given to the affected individuals.

6. **Reporting Requirements**
   When the incident is closed, the lead campus security authority will report to the Associate Vice President for Information Resources and Communications at UCOP:
   - a description of the incident,
   - the response process,
   - the notification process, and
   - the actions taken to prevent further breaches of security.

Figure A – Incident Response/Notification Chart



Attachment B: References

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

Information Security Policy, Business and Finance Bulletin IS-3 (http://www.ucop.edu/ucophome/policies/bfb/is3.pdf)

Misuse of University Resources, UC Davis Policy and Procedures Manual, Section 330-95 (http://manuals.ucdavis.edu/ppm/330/330-95.htm)

Recommended Practices on Notification of Security Breach Involving Personal Information - October 5, 2003. Office of Privacy Protection, California Department of Consumer Affairs. (http://www.privacyprotection.ca.gov/recommendations/secbreach.pdf)