

UNIVERSITY OF CALIFORNIA
INFORMATION SECURITY WORK
GROUP REPORT

August 9, 2005

TABLE OF CONTENTS

I. Executive Summary

II. Background

III. UC Leadership Initiatives to Ensure Information Security

1. Roles, Responsibilities and Accountability for Safeguarding Restricted Data
2. Initiatives to Raise Awareness and Educate the UC Community
3. Comprehensive Information Security Policy and Compliance Programs

IV. Management Initiatives to Safeguard Restricted Data

1. Academic and Administrative Unit Management Activities
2. Information Technology Management Strategies
3. Effective Handling of Information Security Incidents

V. Summary of Major Recommendations

Appendices :

1. Recommended Actions to Protect Restricted Data
2. Sample Campus Communications Regarding Information Privacy and Security
3. Sample Information Security Risk Assessment Blueprint
4. UC Davis Draft Encryption Policy
5. Sample Incident Response Check List
6. The OWASP Top Ten
7. UC Information Security Work Group Members

UC INFORMATION SECURITY WORK GROUP REPORT

I. Executive Summary

Since California's security breach notification law took effect in July, 2004, UC has followed a rigorous set of guidelines for notifying individuals whose personal information may have been acquired as a result of a computer security breach. Many UC campuses have experienced thefts of laptop computers, compromised servers or other events involving unauthorized access to personally identifying information and have notified affected individuals of the possible risks and repercussions of such breaches. Recent security breaches have captured the attention of the media and drawn the anger of many affected individuals. They have also served as catalysts for new proposed state and federal legislation focused on ensuring greater safeguards for personal data and greater accountability for organizations that are stewards of this data.

President Dynes and the Chancellors requested that a University-wide group be formed to assess the effectiveness of UC's current efforts to safeguard personal information and to recommend further initiatives to reduce the number and severity of security breaches in the future. This report summarizes the deliberations and recommendations of the work group, comprised of academic and administrative leaders throughout the University. Although it is not exhaustive of all possible preventive strategies, this report discusses a broad range of actions that the University should take in order to ensure information security and to successfully prevent breaches of restricted information in the future.

Section V summarizes these recommendations, which include:

- Leadership actions to establish roles and responsibilities for information security and to enforce standards of accountability for security breaches
- University-wide and campus-based security education and awareness activities
- Guidelines for effective handling of security incidents
- Stronger information security policies to address minimum connectivity standards and guidelines for allowable use of restricted data
- Campus security programs to ensure required risk assessments and mitigation strategies at the academic and administrative unit level
- Promotion of campus-based data encryption programs

This report will be reviewed at the September Council of Chancellors meeting.

UC INFORMATION SECURITY WORK GROUP REPORT

II. Background

In April, 2005, President Dynes and the Chancellors requested that a University-wide work group be formed to assess UC's current efforts to safeguard restricted data in electronic form, in particular any information that can be used to identify individuals, and to recommend further initiatives to reduce the number and severity of information security breaches experienced by University organizations. The work group explored leadership, educational, policy, technology and other strategies to develop a series of observations and recommendations.

It should be noted that there are security threats to information technology, such as service disruption, that do not involve unauthorized release of restricted information. There are also threats to restricted information in non-electronic form. This report, however, focuses on safeguards for restricted information in electronic form.

Definitions of “Restricted” Data

This report employs the term “restricted” data as it is defined in University of California Business and Finance IS-3, “Electronic Information Security” (IS-3), <http://www.ucop.edu/ucophome/policies/bfb/is3.pdf>. IS-3 applies to all aspects of the University mission and defines *restricted* data as data that is considered restricted to some degree. Two categories of restricted data are defined: *Personal* and *Limited*.

Personal data refers to the combination of any information that identifies and describes an individual, including but not limited to, his or her name, social security number, protected health information (PHI), and financial account information.

Limited data refers to electronic information whose unauthorized access, modification or loss could seriously or adversely affect the University (e.g., cause financial loss or loss of confidence or public standing in the community), adversely affect a partner (e.g., a business or agency working with the University), or adversely affect the public.

III. UC Leadership Initiatives to Ensure Information Security

The University strives to ensure usability and ready access to stored data needed for university objectives while at the same time to secure and protect personal and other kinds of sensitive data that if accessed without authorization can negatively affect an individual or the institution. Balancing this need and the associated risk requires both individuals (faculty, staff and student employees) and units assuming responsibilities for data protection and security. Every member of the University of California has a role to play in securing data that has some degree of sensitivity. Clear roles and responsibilities are a foundation upon which the University can and should articulate professional expectations as well as standards of accountability. Communication of roles and responsibilities and general efforts to raise awareness of information security issues are important leadership actions, as are the development and updating of key policies and guidelines regarding information security. Furthermore, it is important to understand and convey that information security is an exercise in risk management. Units and individuals may adhere to all defined practices and policies and still have a restricted data breach. A breach must be analyzed, good practices recognized, and lessons learned or new approaches incorporated.

While restricted data may reside in all forms of electronic communications, the immediate focus of University-wide efforts to ensure the security of restricted data should be directed to significant *collections of such data* (e.g. spreadsheets, data sets).

1. Roles, Responsibilities and Accountability for Safeguarding Restricted Data

UC Leadership Engagement: University leadership plays a critical role by making direct statements to the campuses, medical centers and labs, discouraging storage of restricted information without need, and emphasizing that restricted data must be protected when it is stored, used or transmitted by academic and administrative units throughout the University. Such statements lead to better understanding of standards of accountability for all employees during the regular discharge of their duties and in the case of security incidents. Establishing accountability involves assigning responsibility for the consequences of a security event. Leadership must support the enforcement of standards of accountability for safeguarding restricted data through employee performance management processes.

Individual responsibilities: All members of the UC community (faculty, staff and student employees) should be required: (1) to identify, to the best of their ability, any restricted data that resides on their individual devices and (2) to comply both with campus requirements regarding the storage of restricted information on these devices and with minimum standards to connect to the campus network. If an individual has a specific requirement to store restricted data on an individual device, certification of compliance with prescribed procedures for protection and use of such data should be required. *See Appendix 1 for a list of Recommended Actions to Protect Restricted Data.*

Unit responsibilities: Units are the highest levels of organizational entity defined within the governance, organization and culture of each campus where actionable responsibility can be assigned. Unit responsibilities include: administering data access policies and permissions, administering and enforcing connectivity standards, assigning responsibility for security programs, maintaining required inventories of protected data, articulating guidelines and practices for protection of information assets, conducting and funding security audits, handling information security incidents and implementing remediation strategies. Central campus IT and IT Internal Audit groups can often provide valuable assistance to the units in these areas. Academic and administrative units are also responsible for incorporating information security focus into their core business processes with requisite communication and training activities.

When a security incident occurs, the unit participates in the incident response process which typically involves the designated campus information security official, IT security officer and external experts (e.g. FBI or forensics specialists) as appropriate. The unit has primary responsibility, in coordination with the designated campus information security official, legal counsel, law enforcement, and external relations specialists, for notifying affected individuals as required under the law and covering the costs of the incident response process. The unit must also ensure that the proper incentives are in place to ensure the timely reporting of security incidents according to University guidelines.

Campus-wide responsibilities: Campuses are responsible for articulating guidelines for information management and use consistent with University-wide policies. Certain responsibilities related to information security practices are defined and managed at the institutional level. Examples include campus network management and identity management frameworks to identify and authorize individuals on campus to access systems and information resources. Campuses should also consider creating a formal data stewardship, protection and management organization including a Chief Security / Privacy Officer. Campus internal controls and risk management professionals should be engaged in strategies to safeguard restricted data in academic and administrative operations. Campus-wide education and communications efforts are also important complements to activities at the unit level.

University-wide responsibilities: In order to take advantage of skilled resources throughout the University, and to ensure that the financial and business reputation risks associated with breaches of restricted data are evaluated at a system wide level, the University should establish and administer an “insurance-like” fund to offset campus liability and prevent punitive disincentives in the case of security breaches involving very significant public notification responsibilities. The University should provide clear guidelines to the campuses for the handling of security incidents. University-wide security audit and forensics teams should also be piloted and made available for dispatch at the request of a campus. UC should establish a data risk management program and function to provide support to the campus units.

2. Initiatives to Raise Awareness and Educate the UC Community

Communications: The University should launch a system wide public relations-style campaign directed to all members of the community, emphasizing both the risks and impacts of failures to adequately protect restricted information sources and the individual responsibilities to ensure effective protection of restricted data.

In addition, campuses, medical centers and national laboratories should communicate regularly to general and specific audiences within their institutions on such topics as guidelines for storage and handling of restricted data, guidelines for data encryption, and minimum security requirements. *Sample Campus Communications Regarding Information Security are found in Appendix 2.*

Education/Training: In order to increase awareness of information security risks and to drive desired behavior within the University, there is a requirement for training for academic and administrative unit administrators and users who work with restricted data. Such training should be designed and delivered via the Web and in a format that will make it easily adaptable to campus learning environments. A certification component should support campus efforts to ensure full participation.

In addition to education for the general audiences within UC, system administrators, programmers, PC coordinators and departmental IT support staff need regular training and professional development on topics related to information security challenges and strategies.

3. Comprehensive Information Security Policy and Compliance Programs

Information Security Policy:

Business and Finance Bulletin IS-3, Electronic Information Security, identifies the set of measures that should comprise campus IT security programs. Recently reissued and expanded in scope to apply to the entire University of California, this bulletin addresses management practices and technological safeguards to be addressed by each University campus. IS-3 recommends security measures based upon the sensitivity or criticality of information resources. Campuses, medical centers and national laboratories should:

- Pursue measures to ensure that IS-3 is actively communicated to all members of the community,
- Ensure that IT security programs consistent with the requirements of IS-3 are fully implemented within their organizations.

IS-3 should be updated to include minimum security requirements, data encryption requirements, standards for allowable use of restricted data on individual devices and guidelines for handling security incidents.

Business and Finance Bulletin IS-10, Systems Development and Maintenance Standards, describes standards for developing (or purchasing and installing and

maintaining computer applications for administrative purposes. The bulletin emphasizes and describes business process planning and management.

Regulatory compliance:

Increasingly, federal and state laws are requiring protection of specific information assets, including, but not limited to data that identifies an individual. In compliance with these laws, the University has established the following implementation policies to guide campuses in their implementation procedures and practices.

- Information Practices Act of 1977
 - RMP-8: [Legal Requirements on Privacy of and Access to Information](http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html)
<http://www.ucop.edu/ucophome/policies/bfb/rmp8toc.html>
 - [Applicability of RMP-8 to Student Records: LTR041905-rpm8 \[1\].PDF](#)
 - http://atyourservice.ucop.edu/employees/policies/staff_policies/spp80.htm
 - [APM 160-20: Access to Academic Personnel Records](http://www.ucop.edu/acadadv/acadpers/apm/apm-160.pdf)
<http://www.ucop.edu/acadadv/acadpers/apm/apm-160.pdf>
- California Law About Notification in Instances of Security Breaches, effective July 1, 2003, California Civil Code Section 1798.29;
 - <http://www.ucop.edu/irc/itsec/securitybreach.html>
- FERPA: Disclosure of student records
 - <http://www.ucop.edu/ucophome/coordrev/policy/4-25-02.html>
 - <http://www.ucop.edu/ucophome/coordrev/ucpolicies/aos/toc130.html>
 - RMP-11 Student Applicant Records
<http://www.ucop.edu/ucophome/policies/bfb/rmp11.html>
- Financial Modernization Act (G-L-B): UC Information Security Program
 - http://www.ucop.edu/irc/itsec/uc_info_security.pdf
- Health Insurance and Portability and Accountability Act
 - <http://www.universityofcalifornia.edu/hipaa/welcome.html>

IV. Management Initiatives to Safeguard Restricted Data

1 . Academic and Administrative Unit Management Activities

Standard management practices in academic and administrative units and departments must incorporate appropriate information security measures to ensure a stable and secure technological environment.

Information Security Risk Assessment: An information security risk assessment is a careful examination of where restricted data resides in and how it moves through your work environment and business processes. It is intended to evaluate if the unauthorized disclosure of this information could cause harm to people or to the institution and to identify the precautions that should be taken to prevent it.

Successful information security risk assessments require full support of senior management and must be conducted by teams that include both functional managers, internal audit and departmental and central IT administrators as required. As business operations, workflow, or technologies change, periodic reviews must be conducted to analyze these changes, to account for new threats and vulnerabilities created by these changes, and to determine the effectiveness of existing controls. Campus Controllers and Offices of Internal Controls and Accountability routinely provide risk assessment tools and methodologies to assist departments. *A Sample Information Security Risk Assessment Blueprint is provided in Appendix 3.*

a. Location and transmission of restricted data

Units must identify all resources that may be used to store or transmit restricted data. This inventory must take into account not only the permanent location of data, but also any temporary storage of data, such as laptops, PDAs or other portable devices. Back-up systems must also be included in the risk assessment inventory. Examination of data transmission should include a list of network protocols that are used to exchange, send, or receive data.

b. Identification of threats and vulnerabilities

Threats are events or actions (e.g. power failure, hardware/software failure, data destruction, a compromised machine) that exploit a vulnerability to attack an asset and cause harm as a result. Vulnerabilities can be identified by examining the following in your data collection process: physical security environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc. Campuses should engage knowledgeable and trained data security experts to conduct periodic tests of the vulnerability of databases, particularly those that are accessible via the Internet. UC should consider creating or should contract with external organizations to offer the services of team of “ethical hackers” to identify campus restricted database vulnerabilities.

Implementing Information Security Plans: After completing the risk and vulnerability assessment process, the department or unit must develop an information

security plan that identifies an acceptable level of risk and cost-effective strategies to address that risk consistent with their business goals and activities. The plan should outline the processes and controls that will be implemented to enhance security.

a. Rights of access to restricted data

Only those individuals who have a legitimate business reason to access or use restricted data should be allowed access to that data. The security plan must identify an authorization process that identifies those individuals and determines the type of access allowed (e.g., read-only, create, delete, and/or modify) consistent with policy.

b. Strategies to protect restricted data

Protection of restricted data must include both logical (technical) and physical security measures. These include measures for controlling authorized access, such as appropriate authentication measures, and implementation of technical and physical solutions.

c. Security awareness training

The security plan must include a training plan to ensure that each member of the unit or the department is informed regarding the recommended procedures established by the unit or department. Where regulation requires certification, departments shall establish a mechanism to provide proof-of-training, including required records. Procedures must also ensure training of newly-hired staff.

Monitoring the effectiveness of the security plan: Routine testing, monitoring, and evaluation of safeguards implemented in security plans must be conducted on a periodic basis to minimize potential unidentified risks.

Handling security incidents: Departmental security incident handling procedures should include identification of personnel to be alerted when a possible security incident has been detected. Individuals who are assigned this responsibility must coordinate with the campus incident response team to ensure appropriate analysis and response.

Securing UC restricted data used in operations with external business partners, agents or affiliates: When passing restricted data to an agent of the University, there must be a written contractual agreement in place for all agreements (including terms and conditions) that:

- Prevents disclosure of restricted data by the agent or affiliate to other third parties including subcontractors,
- Requires all agents and affiliates to observe federal and state laws and UC policies for privacy and security,
- Requires a specific plan by the agent or affiliate for the implementation of logical, physical, and managerial security strategies,

- Requires a plan for the destruction of restricted data upon completion of the agent's or affiliate's work for UC.

2. Information Technology Management Strategies

University IT leadership must provide secure, reliable applications and tools to support the broad range of activities related to the University's mission. A secure environment includes proper management of applications which use restricted data as well as management of the technology infrastructure (servers, desktops, laptops, PDAs, smart phones, etc.). In addition, network technologies can be used to augment these protections. (See Appendix 1: Recommended Actions to Protect Restricted Data.)

The University's Electronic Information Security (IS-3) policy outlines general requirements and guidelines for University faculty and staff who access or use restricted data to ensure that all precautions are taken to secure this data and the environment in which it resides. Of particular importance are:

Encryption Strategies: Encryption is a technique for protecting information from unauthorized access when sufficient physical security cannot be provided. Encryption must be used in the following situations:

- When restricted information is transmitted across a network that has not been specifically engineered to provide a sufficient level of security.
- When restricted information is stored on a device (such as a laptop, smart phone, or CD-ROM) for which sufficient physical security cannot be provided. Note that many desktop and server systems are also not in secure environments with strong physical access controls and, therefore, will require storage encryption. Risk assessment should consider the impact of equipment theft and other security breaches *vs.* the cost of implementing encryption for all devices holding restricted information.

An important component of campus encryption strategies is the management and protection of encryption keys. IS-3 provides criteria to ensure that encrypted information remains secure, while ensuring that authorized access is not impacted due to loss of keys.

Note that, while a powerful tool, encryption is not a cure-all for security issues. A careful analysis of information flow is needed to determine encryption's feasibility and applicability. *The UC Davis Draft Encryption Policy is included in Appendix 4.*

Minimum Standards for Connectivity to the Campus Network: All campuses should establish minimum connectivity standards, provide reasonable notice to members of the campus community and disconnect or limit the connectivity of machines and servers that do not comply with such standards.

Minimization of Restricted Data Resident on Campus Storage Devices: All campuses should establish policies that minimize the restricted data resident on any machine or storage device.

Network Management Tools and Services: Network management tools and services should be employed, where appropriate, to enhance application and system security. Such tools and services include firewalls, Intrusion Detection Systems, network vulnerability scanning and Virtual Private Networks. IT staff responsible for vulnerability testing require ongoing training to ensure that up-to-date approaches are being employed. Systemwide training sessions would help to reduce overall training costs.

Logging Strategies for Intrusion Detection and Forensic Analysis: Two significant challenges in IT security are: 1) understanding when an incident has occurred and 2) performing the forensic analysis necessary to determine the scope and magnitude impact of the incident. Many components of the technology environment generate transaction logs which can be invaluable during these activities. In order to ensure the value of this information, the University should develop a strategy for log management that includes:

- retention schedules and tools for discarding old information
- secure storage of the information
- analysis tools
- routine inspection of log data

Authentication and access controls: Appropriate authentication and access controls must be employed to assure that only authorized people gain access to restricted information and the systems that maintain that information.

Backup and recovery: Backup and recovery procedures must exist and be tested regularly. The backup media containing restricted information must be physically secure and/or encrypted.

Systems maintenance and development: Robust systems management must be employed for applications and systems that maintain restricted information. These practices include (but are not limited to): anti-virus and security patch management, closing ports, shutting down unused services and operating change monitoring tools. Appropriate software development practices must be employed for these applications, as described in IS-10. Resources, such as the Open Web Application Security Project (OWASP – <http://www.owasp.org>), should also be consulted. *See Appendix 6 for the OWASP Top Ten Most Critical Web Application Security Vulnerabilities.*

Service protection: Applications and their underlying computing devices should employ firewalls to protect them from unauthorized network access. This protection should be implemented at both the system level and within the network.

3. Effective Handling of Information Security Incidents

Effective handling of a security breach requires preparation and planning well in advance of the breach itself. The University should:

Establish standard incident response procedures: The University should define a standard incident response process that can be adapted to different campuses. Incident response procedures will exist at multiple levels through the organization and are dependent on the information and resources involved. Campuses and medical centers should notify UCOP (AVP-Information Resources and Communications) of all security incidents involving breaches of restricted data. *See Appendix 5 for a Sample Incident Response Checklist.* The incident response process should communicate:

- the people who should be involved
- provisions to protect forensic information before restoring service
- conditions that may require public disclosure

Determine the extent of breaches once they have occurred: Post-security breach investigation and notification require specialized technological and forensics skills. Departmental and central campus IT organizations typically offer such resources to support the units. While some campuses may choose to develop this capability in-house, others may contract with external service providers.

The University should:

- Develop local and system-wide teams to oversee the investigation process
- Develop standing agreements with companies, e.g. Guidance Software, for use of their forensic services where appropriate.
- License forensic software tools, such as EnCase, Vericept and Silent Runner, in addition to utilizing the open source tools that are available.
- Review guidelines for determining when notification to individuals affected by a security incident is required

Establish relationships with appropriate law enforcement agencies: The University should ensure that law enforcement agencies continue to be an integral part of the planning for incident response. In particular, understanding when and how to engage law enforcement can greatly facilitate the forensics investigation process at the time of a breach. Note that this will likely result in training requirements within campus law enforcement units.

V. Summary of Major Recommendations

1. Leadership

Develop system-wide and campus guidelines to ensure compliance with standards of accountability for data security breaches.

RESPONSIBLE PARTY: Chancellors or their designates

2. Communications

University-wide: Develop a UC wide communication campaign (including message from President)

RESPONSIBLE PARTY: UCOP Strategic Communications

UCOP / Campus: Create templates for general campus communications and communications targeted to specific communities.

RESPONSIBLE PARTY: IT Leadership Council (ITLC) with Campus Communications

3. Information Security Training

Create a Web-based training module for general purpose use by UCOP, the campuses and medical centers. Explore and recommend certification options.

RESPONSIBLE PARTY: Work group (to be formed) with campus training and development experts and UC Information Technology Policy and Security (UCITPS) members to recommend a WEB-based training program

4. Handling of Security incidents

- Communicate guidelines for log management activities and identify appropriate tools for use by campuses

RESPONSIBLE PARTY: UCITPS group and Director, Advanced Technology with ITLC

- Contract for forensics tools and services on a system wide basis

RESPONSIBLE PARTY: IT Strategic Sourcing Program with the ITLC

- Create University-wide security audit and forensics teams to assist campuses at their request

RESPONSIBLE PARTY: ITLC with UC Internal IT Audit team

5. Policy Updates

Update UC Electronic Information Security (IS3) to include:

- General UC-wide guidelines for security incident handling
- The roles, responsibilities and accountability for information security framework included in this report
- Minimum network connectivity standards for both general use computers/servers and devices that store sensitive data
- Guidelines for encryption of restricted data
- Standards for allowable use of restricted data
- RESPONSIBLE PARTY: ITLC, UCITPS

6. Campus security programs

- Identify a responsible party on each campus for development and oversight of campus information security programs required in IS-3
- Develop campus security programs, including local campus policies and guidelines for ensuring compliance
- RESPONSIBLE PARTY: Campus CIO or ITLC member or designated responsible person assigned by the Chancellors

7. Encryption

- Promote the development of campus-wide storage encryption services with requisite technologies, authorizations and cryptography infrastructure
RESPONSIBLE PARTY: Campus CIO or ITLC member or designated responsible person assigned by the Chancellor
- Select and contract for encryption tools and technologies on a system wide
- RESPONSIBLE PARTY: UCOP Director Advanced Technology, UCOP Director, Clinical Services Development, ITLC

APPENDICES

- 1. Recommended Actions to Protect Restricted Data**
- 2. Sample Campus Communications Regarding Information Privacy and Security**
- 3. Sample Information Security Risk Assessment Blueprint**
- 4. UC Davis Draft Encryption Policy**
- 5. Sample Incident Response Check List**
- 6. The OWASP Top Ten**
- 7. UC Information Security Work Group Members**

Appendix 1: Recommended Actions to Protect Restricted Data

Any individual who has possession of restricted information becomes an *Electronic Information Resource Custodian* under IS-3 (Electronic Information Security). Such individuals are accountable, in conjunction with their departmental and campus IT support organizations, for assessing the security risks associated with this information and for implementing appropriate controls to protect it. Additional requirements for safeguarding restricted data may be dictated by federal or state legislation such as HIPAA or by industry requirements for consumer data protection, such as Payment Card Industry (PCI) Data Security Standards.

Following are recommended actions for individuals to safeguard restricted data and information:

- **Avoid storing restricted data on desktop and portable devices.** If restricted data must be transferred onto portable devices, immediately implement measures, such as encryption, to safeguard the confidentiality or integrity of the data in the event of theft or loss of the portable device.
- **Maintain appropriate physical security for computing devices** with restricted data. Take special care with mobile devices, such as laptops, smart phones, and USB “thumb” drives that store restricted data.
- **Determine the level of confidentiality of the information you handle** by consulting privacy, security, and records retention policies and follow departmental procedures for handling departmental information.
- **Remove all information from your old computer when you replace it.** Be aware that many types of erased data can be recovered from your computer, unless you take explicit measures to effectively remove it.
- **Notify third parties that data is restricted and requires security protection** when personally identifying information is distributed to others. Include reference to applicable policies and regulations. Delete personal information not critical to the task when distributing full data sets.
- **Employ safe practices when using your personal computing devices** (*e.g.*, desktop systems, laptops, PDAs, smart phones, *etc.*). For example:
 - Use appropriate authentication and access controls.
 - Keep your software up-to-date.
 - Run anti-virus and anti-spyware software.
 - Be careful when browsing the web, downloading programs and opening e-mail attachments. Sources of unsolicited information, such as advertising pop-ups and spam often contain links to malware and

should be avoided. Use safer browser software, such as Firefox or Opera, unless browsing to a site that requires Internet Explorer.

- Control physical access to your machine.
- Routinely back up files on your system.
- Turn your computer off when you leave for the day.
- Install screen-saver passwords.
- Recognize that personal and shared “network drives” on file servers may not provide the controls required for restricted information. Work with your computing support organization when assessing the associated risks.

Appendix 2: Sample Communications Regarding Information Privacy and Security

Following are four examples of campus communications regarding information security.

SUBJECT: Laptop and Other Mobile Device Security - Securing Private Information

TO: ALL ACADEMICS AND STAFF AT CAMPUS / MEDICAL CENTER

If you are utilizing the CAMPUS network or have CAMPUS -related data on your laptop or other portable devices, you are responsible for its safekeeping just as if you were working at your desk on campus. As a member of the CAMPUS community, you may have responsibility for some processes that include access to private information: Social Security numbers, birth dates, home phone numbers, location of assets, credit card numbers, HIPAA, FERPA, etc. The use and protection of much of this information is governed by federal and state law/regulation and university policy. Therefore, if you use and/or store private information as described above, you should examine the business processes you undertake for the university and ensure that the retrieval/storage of private information on any portable devices you use is essential for such processes.

You need to take extra precautions with the physical security of such devices to ensure they do not get taken by unauthorized people. The link below provides additional information regarding this topic and will provide you with steps you need to take to ensure you are doing all that you can to protect the university data. Insert CAMPUS URL HERE.

All members of the university community are obligated to respect and protect private information whether it is transmitted and stored electronically (e.g. e-mail) or in hardcopy. It is important to understand that each individual is responsible for the information under his or her control. Responsibility for protecting individual privacy is a part of everyone's job.

II. SUBJECT: Minimum Network Security Requirements

TO: ALL ACADEMICS AND STAFF AT CAMPUS / MEDICAL CENTER

CAMPUS depends on its information technology infrastructure to support its research, instruction, healthcare and administrative systems. This infrastructure is under constant attack: hackers are attempting to break into computers across campus every day. Even more dangerous and costly threats loom as viruses become increasingly malicious and hackers become more sophisticated.

To combat this threat we have jointly approved a set of minimum security standards to be met by any device connected to the CAMPUS network. The Academic Senate Committee on Academic Information Technology has also endorsed these standards.

The minimum standards and how to implement them are listed in the Implementation Guide (see below) and include:

- Anti-virus software
- Firewall protection

We encourage you to implement these standards as soon as possible. Devices that have not met the new standard by the DATE will be subject to disconnection from the CAMPUS network. Exceptions to the minimum standards will be approved on a case-by-case basis and only if network security is not jeopardized.

Anti-virus tools are available at no charge to the CAMPUS community for both campus and home use. A variety of anti-virus tools are acceptable for the purposes of meeting the minimum standards. Host-based firewall protection is included in current versions of the major supported operating systems (Windows XP and Mac OS X). Instructions for configuring and enabling these and other OS versions can be found in the CAMPUS Network Security Resources link.

Computer users should check with their system administrators to see if their machine(s) are already policy-compliant and, if not, what steps need to be taken to make them compliant. Computer users who serve as their own system administrators are responsible for bringing their devices into compliance with policy, using the instructions provided on the websites below. Additional help may be available from departmental and/or divisional computing staff.

Administrative officials should review the Network Security Policy, which contains the minimum standards to be met to determine the impact on their unit and to ensure that steps are taken to comply. Information concerning implementation of the minimum standards is available on the websites below. System administrators should review the Network Security Policy and bring any noncompliant machines into compliance.

III. SUBJECT: Your Responsibility for Securing Private Information

TO: ALL FACULTY AND STAFF AT CAMPUS / MEDICAL CENTER

As a member of the CAMPUS community, you may have responsibility for some processes that include access to private information, such as Social Security numbers, birth dates, home phone numbers, location of assets, credit cards, student data, patient records, etc. A message on the same topic was sent to you a few months ago (see URL). The use and protection of much of this information is governed by federal/state law and by university policies. All members of the university community are obligated to respect and protect private information, whether it is transmitted and stored electronically (e.g.

e-mail) or in hardcopy. It is important to understand that each individual is responsible for the information under his or her control.

Therefore, if you use and/or store private information, you should examine your businesses processes and ensure that the retrieval/storage of private information is absolutely necessary. In addition, you should be able to answer the following statements affirmatively:

1. Access to all private information I work with is restricted on a "need-to-know" basis.
2. Access to my computer and other information technology equipment assigned to me is password-protected.
3. I log off my computer or use a screensaver password when I leave my workstation.
4. Information on my screen is kept hidden from visitors to my work area.
5. All sensitive papers, printouts, etc., are safely secured during the day when I leave my work area and locked up during non-work hours.
6. My computer has up-to-date anti-virus software, firewall, and software patches.

Additional information may be found at: [CAMPUS URL'S](#)

IV. SUBJECT: CAMPUS Policy on Use and Storage of Sensitive Electronic Data

TO : BUSINESS ADMINISTRATION UNIT

Dear Colleagues,

As you know, we will be fully engaged in assessing the safety and security of our computer systems, networks and workstations over the next few months. While that extensive effort will serve us well in the future, there are some immediate steps we must take pending that longer term assessment.

In light of the recent increase in incidents across the UC system where sensitive data may have been compromised as a result of stolen laptops and/or hacking, I am implementing a new policy for all CAMPUS / DIVISION units as follows:

Effective immediately, no restricted information is to be downloaded or stored on any of the following:

- Any local workstation computer including laptop computers
- Home computers
- PDAs, Blackberries, or other mobile devices
- Removable media other than secured departmental back up tapes or secured archives.

The deletion and removal of all restricted information from the above should be completed no later than DATE. I will ask that you report back to me when this is completed and if you need any additional help or support to accomplish this that you contact NAME.

For the purposes of the above, restricted information is defined in CAMPUS Policy NUMBER as “personal name along with social security number, California driver identification number or financial account information”. This policy applies to:

- all UNIT staff including part time and temporary employees;
- employees of temporary agencies and contractors used by CAMPUS units;
- all devices noted above, used for University business, whether or not they are owned by the University.

Employees who violate this policy may be subject to disciplinary action up to and including dismissal. Although this is a harsh statement, the responsibility we have as stewards of this personal identity information and the very negative consequences to individuals who have their identities stolen requires that we take this very seriously.

Instances of criminal acts of identity theft are on the rise and workstations and personal devices that house personal information can be vulnerable to attack and disclosure of that information. The recently identified thefts of laptops from CAMPUS are resulting in significant costs to the University for the investigation and notification of individuals whose identity data may have been compromised.

While there may be some disagreement with the policy to delete any and all files on workstations, laptops and personal devices, I can think of no compelling business reason where we would put the campus community at risk by such practices. However, if you have a compelling business reason for requesting an exception, please discuss those with NAME and we will evaluate the risk on a case by case basis.

Please review your use of any departmental workstations and laptops, PDAs, home computers (if used for work), removable media, and local hard drives to make sure they do not contain files with this kind of data. If they do, please have the files deleted immediately.

Please consider carefully the files and electronic messages that you work with—both those that you worked with recently as well as old files that are still stored on the above devices. Those may include:

- Saved files of performance evaluations that, prior to the use of employee ID number, included both employee name and social security number;
- Radiation worker information and radiation dosimetry results that contain name and social security number;

- Data related to DMV pull notices that contain names and California drivers license numbers;
- Downloads from CAMPUS FINANCIAL SYSTEM, PPS or CAMPUS STUDENT INFORMATION SYSTEM;
- Messages and Contacts in Outlook;
- Messages on older e-mail systems such as Eudora;
- Specialty systems like Paradox, CheckImage, AlienTax or PropertyTax;
- Any and all other programs you use to store files and messages.

Finally, within the UNIT , we deal on a daily basis with a variety of confidential data that, while falling outside of the CAMPUS policy definition of “personal data” must continue to be treated with care and maintained in confidence (e.g., birth date or home address). Care must also be exercised if you are faxing or scanning any type of confidential data to make sure that the person or entity you are sharing this confirmation with has a legitimate business need for the data and is taking the necessary precautions to ensure the data is adequately protected.

I know that we have always taken great care in safeguarding data. We will need to remain vigilant about this difficult and evolving responsibility at all levels and continue appropriate and timely steps to safeguard this data.

Appendix 3: Sample Information Security Risk Assessment Blueprint

These following guidelines offer a simple step-by-step process. Additional resources and methodologies are listed under Resources below to help you establish an approach appropriate to your environment.

General Guidelines for an Information Security Risk Assessment

- 1. Establish the risk assessment team.** The risk assessment team will be responsible for the collection, analysis, and reporting of the assessment results to management. It is important that all aspects of the activity work flow be represented on the team, including human resources, administrative processes, automated systems, and physical security.
- 2. Set the scope of the assessment activity.** The assessment team should identify at the outset the objective of the assessment project, department, or functional area to be assessed, the responsibilities of the members of the team, the personnel to be interviewed, the standards to be used, documentation to be reviewed, and operations to be observed.
- 3. Identify information assets covered by the assessment.** Assets will include any data or information that contains information characterized as “restricted” in the University’s Electronic Information Security (IS-3). Also included are personnel, hardware, software, data (including classification of sensitivity and criticality), facilities, and current controls that safeguard those assets. It is important to identify all assets deemed to be in scope of the assessment project.
- 4. Categorize potential impacts of loss of or damage to an asset:** Losses may result from physical damage, denial of service, modification, unauthorized access, or disclosure. They may be intangible, such as the loss of the organizations' credibility.
- 5. Identify threats and vulnerabilities.** A threat is an event, process, activity, or action that exploits a vulnerability to attack an asset. Include natural threats, accidental threats, human accidental threats, and human malicious threats. These could include power failure, biological contamination or hazardous chemical spills, acts of nature, or hardware/software failure, data destruction or loss of integrity, sabotage, or theft or vandalism. A vulnerability is a weakness which a threat will exploit to attack the assets. Vulnerabilities can be identified by addressing the following in your data collection process: physical security, environment, system security, communications security, personnel security, plans, policies, procedures, management, support, etc.
- 6. Identify existing controls.** Controls are safeguards that reduce the probability that a threat will exploit a vulnerability to successfully attack an asset. Identify those safeguards that are currently implemented, and determine their effectiveness in the context of the current analysis.
- 7. Analyze the data.** In this phase, all the collected information will be used to determine the actual risks to the assets under consideration. A technique to

analyze data includes preparing a list of assets and showing corresponding threats, type of loss, and vulnerability. Analysis of this data should include an assessment of the possible frequency of the potential loss.

- 8. Determine cost-effective safeguards** (See Control Safeguards below). Include in this assessment the implementation cost of the safeguard, the annual cost to operate the safeguard, and the life cycle cost of the safeguard.
- 9. Report.** The type of report to make depends on the audience to whom it is submitted. The report should include findings; a list of assets, threats, and vulnerabilities; a risk determination, recommended safeguards, and a cost benefit analysis.

Control Safeguards

1. Administrative Safeguards

These include, but are not limited to, those control measures that ensure:

- classification of data handled by the unit and determination of controls to protect those assets;
- documentation of procedures, standards, and recommended practices to ensure that applicable policies and controls are implemented appropriately for a given business process;
- identification of personnel who are authorized to access systems;
- assurance that appropriate authorization controls are implemented;
- security awareness training and education for all personnel; and
- background checks prior to the selection and hiring of new personnel into critical positions.

2. Technical (Logical) Safeguards

These encompass the range of technical controls that:

- ensure access by only authorized users and session termination when finished;
- enforce secure password management;
- manage tracking of development, maintenance, and changes to application software and information systems;
- manage access to the network; and
- ensure event logging.

3. Physical Safeguards

These protect physical resources through controls that

- allow access by only authorized individuals, through the use of physical means, such as locks, badge readers, or access cards;
- ensure the prevention, detection, early warning of and recovery from emergency disruptions, such as flooding, power failures, or earthquakes; and
- govern the receipt and removal of hardware and electronic media, including equipment reassignment, and final removal of data and disposition of equipment.

Resources

ASIS International: General Security Risk Assessment Guideline
<http://www.asisonline.org/guidelines/guidelinesgsra.pdf>

Department of Health and Human Services: CMS Information Security Risk Assessment (RA) Methodology
http://csrc.nist.gov/fasp/FASPDocs/risk-mgmt/RA_meth.pdf

EDUCAUSE: Effective Security Practices Guide
<http://www.educause.edu/EffectivePracticesandSolutionsinSecurity/1246>

NIST: Security Self-Assessment Guide for Information Technology Systems
<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>

ECAR/Burton Study: A Systematic, Comprehensive Approach to Information Security
<http://csrc.nist.gov/publications/nistpubs/800-26/sp800-26.pdf>

IR&C: Guidelines for conducting risk assessments and security reviews
<http://www.ucop.edu/irc/itsec/risk.html>
<http://www.ucop.edu/irc/itsec/securityreview.html>

Appendix 4: Draft Encryption Policy (UC Davis Policy and Procedure Manual May 2005)

I. Purpose and Scope

Encryption supports data privacy and integrity by providing a method to convert electronic information into a format that is only readable only by authorized individuals. This policy establishes that use of encryption for electronic information in storage shall be consistent with the campus need for continued availability of the information. This policy applies to academic and administrative electronic information in storage and its users.

II. Definitions

The UC Davis Electronic Communications Policy (PPM 310-16) defines terms used in this policy. Additional terms are defined here:

- A. Restricted electronic information – Electronic information for which content requires protection from unauthorized read, modify and/or delete functions. Restricted electronic information includes but is not limited to personally identifiable information protected by federal or state law and information, which if subject to unauthorized access, modification or deletion, could adversely affect the university.
- B. Cryptography – a method used to encode information so that only authorized individuals can read the information
- C. Electronic Storage Media – Electronic storage system used to record, index, store, preserve, or retrieve data files, including portable storage systems.
- D. Encryption – Transforming information using a secret key so that the information is unintelligible to unauthorized parties.
- E. Key escrow – mechanism that permits an authorized third party to decrypt files.

III. Encryption Policy

- A. File encryption must be used to secure restricted electronic information stored on desktop, laptop and server computers and electronic storage media for which physical security controls are limited.
- B. Authorized access to encrypted university information must be preserved. Access by other than the data custodian will be administered under the provisions of the Electronic Communications Policy.
- C. A campus department head must authorize use of file encryption (excluding file transport mechanisms).
- D. The campus unit use of file encryption services must use the campus infrastructure cryptography service. Exceptions must be approved by the campus Information Security Coordinator.

IV. Responsibilities

- A. Users and System Administrators
 - Identify sensitive/restricted information subject to encryption
 - Safeguard encryption security pass-phrases and/or authentication devices

- Use encryption consistent with university policy
- B. Campus Department Head
 - Approve use of encryption within unit
 - Approve information subject to encryption services
 - Ensure cryptography use is consistent with campus and university policies
 - Authorize use of key escrow service to access encrypted files, consistent with university privacy policies.
- C. Information Security Coordinator
 - Develop, maintain and publish cryptography infrastructure standards
 - Develop, maintain and publish list of cryptography products compatible with encryption infrastructure
 - Approve cryptography use which departs from campus infrastructure service or standards
 - Approve campus unit use of key escrow/recovery services to access encrypted files
- D. Information and Educational Technology
 - Develop, administer and maintain hardware and software supporting cryptography infrastructure
 - Publish resources for the use of cryptography infrastructure

V. References and Resources

- A. Information Systems Bulletin 3, Business and Finance Bulletin, University of California
- B. Electronic Communications Policy, PPM 310-16, University of California, Davis
- C. Privacy of and Access to Information, PPM 320-20, University of California, Davis
- D. Cyber-safety Program Policy, PPM 310-22, University of California, Davis
- E. Physical Security Checklist, <http://security.ucdavis.edu/cybersafety.cfm>

Appendix 5: Sample Incident Response Check List

Campus incident response procedures will vary to some extent, depending on the organization of the business functions, information technology, public information, law enforcement, *etc.* In general, all incident response procedures would include the following elements.

- **Ensure that the right people are involved.** At a minimum, the incident response team includes: the affected system's proprietor and custodian, the campus IT security and policy officers, the campus Chief Information Officer, and the Associate Vice President – Information Resources and Communications (UCOP) if public disclosure is required. In some circumstances, other campus experts may need to be involved (e.g. Chancellor's office, campus police, legal counsel, public affairs, risk management, internal audit, the campus payment card coordinator, the campus HIPAA security officer, or national and international IT security organizations (*e.g.*, the US CERT).
- **Secure the area.** Electronic evidence can be very perishable and can be easily destroyed resulting in an inability to prosecute or inability to determine if personal information was compromised. Secure the scene and all the persons on the scene, then visually identify potential evidence, both conventional (physical) and electronic, and determine if perishable evidence exists. Take care not to alter the condition of any electronic device: If it is off, leave it off. If it is on, leave it on. Inventory and evaluate the scene and then formulate a plan.
- **Incident Response Process Steps:** Incident response processes are unpredictable. For this reason, proper documentation at every stage in the process is essential.
 1. **Notify.** Provide initial notification of the breach to the affected system's proprietor and custodian, the campus IT security and compliance/policy officers, and any other people required by the circumstances. Provide updates as appropriate throughout the incident response process.
 2. **Assess the need for forensic investigation.** The factors to consider include the potential value of forensic information *vs.* the immediate need to protect and restore University resources and services. It may be necessary to delay subsequent steps until an appropriate criminal investigation has been conducted.
 3. **Regain control.** Once required forensic information has been collected, regain control of the compromised system. This may include network disconnection, process termination, a reboot, *etc.*
 4. **Analyze the intrusion.** Understand the nature of the intrusion and its impact on information and process integrity. Determine if restricted information may have been acquired by unauthorized individuals. Determine what address information is available for individuals whose data may have been acquired by unauthorized individuals. Estimate the potential cost of the intrusion to the University. (A cost estimate may be required to involve law enforcement.)

5. **Document results of analysis.** Prepare a report on the nature of the incident, the nature of the information that has been compromised, the numbers of individuals affected, address information on impacted individuals, and potential cost to the University.
6. **Submit report.** Notify the campus IT leadership, executive managers, legal counsel, and the Associate Vice President – Information Resources and Communications if there is a possibility that public disclosure will be required.
7. **Recover from the intrusion.** Perform whatever steps are needed to restore the integrity of the affected information and processes.
8. **Correct system or application vulnerabilities.** Correct the condition that allowed the intrusion to occur.
9. **Restore the service.** Once everything is complete, service can be restored
10. **Assemble team to determine if notification is required.** Work with executive management to determine whether to make public disclosures. “Determining the Threshold for Security Breach Notification” (http://www.ucop.edu/irc/itsec/security_breach_notification.pdf) contains issues that should be considered when evaluating the incident and determining whether to notify affected individuals in compliance with California’s security breach notification requirement. Campus counsel and public affairs should be included in the determination evaluation.
11. **Notify.** Ensure notification of the incident's final resolution to the affected system's proprietor and custodian, the campus IT security and compliance/policy officers, the campus IT leader, the Associate Vice President – Information Resources and Communications, and any other individuals who should be engaged in this process.

Appendix 6: The OWASP Top Ten

The Open Web Application Security Project (OWASP – <http://www.owasp.org>) maintains a repository of standards and best practices for secure web-based applications. Their Top Ten Most Critical Web Application Security Vulnerabilities is reproduced here.

OWASP Top Ten Most Critical Web Application Security Vulnerabilities		
A1	Unvalidated Input	Information from web requests is not validated before being used by a web application. Attackers can use these flaws to attack backend components through a web application.
A2	Broken Access Control	Restrictions on what authenticated users are allowed to do are not properly enforced. Attackers can exploit these flaws to access other users' accounts, view sensitive files, or use unauthorized functions.
A3	Broken Authentication and Session Management	Account credentials and session tokens are not properly protected. Attackers that can compromise passwords, keys, session cookies, or other tokens can defeat authentication restrictions and assume other users' identities.
A4	Cross Site Scripting (XSS) Flaws	The web application can be used as a mechanism to transport an attack to an end user's browser. A successful attack can disclose the end user's session token, attack the local machine, or spoof content to fool the user.
A5	Buffer Overflows	Web application components in some languages that do not properly validate input can be crashed and, in some cases, used to take control of a process. These components can include CGI, libraries, drivers, and web application server components.
A6	Injection Flaws	Web applications pass parameters when they access external systems or the local operating system. If an attacker can embed malicious commands in these parameters, the external system may execute those commands on behalf of the web application.
A7	Improper Error Handling	Error conditions that occur during normal operation are not handled properly. If an attacker can cause errors to occur that the web application does not handle, they can gain detailed system information, deny service, cause security mechanisms to fail, or crash the server.
A8	Insecure Storage	Web applications frequently use cryptographic functions to protect information and credentials. These functions and the code to integrate them have proven difficult to code properly, frequently resulting in weak protection.
A9	Denial of Service	Attackers can consume web application resources to a point where other legitimate users can no longer access or use the application. Attackers can also lock users out of their accounts or even cause the entire application to fail.
A10	Insecure Configuration Management	Having a strong server configuration standard is critical to a secure web application. These servers have many configuration options that affect security and are not secure out of the box.

Appendix 7: UC Information Security Work Group Members

Jacqueline Craig, Director, UCOP
Jim Davis, Associate Vice Chancellor, UCLA
Joy Grosser, Chief Information Officer, UCI Medical Center
Kristine Hafner, Associate Vice President, UCOP
Karl Heins, Internal IT Audit Director, UCOP
Andrew Kahng, Professor, UCSD
Jack McCredie, Chief Information Officer, UCB
Stan Nosek, Vice Chancellor, UCD
Bob Ono, IT Security Coordinator, UCD
Steve Relyea, Vice Chancellor, UCSD
Jim Sandoval, Vice Chancellor, UCR
Maria Shanle, University Counsel, UCOP
Scott Sudduth, Assistant Vice President, Federal Government Relations
Carl Tianen, Information Security Officer, UCSF
David Walker, Director, UCOP
Alan Wyner, Dean, UCSB