

University of California
Campus Advisories for Policy on Stewardship of Electronic Information Resources
Draft April 19, 2007: For Comment Only

1. Introduction

This Guide supports the University Policy on Stewardship of Electronic Information Resources. Its purpose is to provide guidance to assist campus managers, faculty, and staff in the implementation of their information management strategies. It also offers references to existing related University policies, guidelines, and resources.

- See Appendix A for a list of related University policies, guidelines, and resources.

2. Confidentiality

The University of California respects the privacy of the members of the University community and has established policies and procedures consistent with federal and California law to guide the conduct of University activities relating to confidential information.

- The [Records Management and Privacy](#) website contains Business and Finance Bulletins that provide guidelines for disclosure and release of information about individuals and guidelines for University records management.
- See [Policies Applying to Campus Activities, Organizations, and Students, section 130.00](#) for guidelines governing privacy of student information.
- See [Academic Personnel Manual, section 160](#), for a description of the privacy rights of academic employees.
- See [Electronic Communications Policy](#) for policy and procedures regarding the examination, monitoring, or disclosure of personal electronic communications records.
- See [UC HIPAA website](#) for guidelines regarding the privacy and protection of health information.

3. Electronic Information Management

A. Information Management Planning

A fundamental element in information management is the advance thinking about possible mishaps or events that would result in loss or damage to data, impair regular functionality, or prevent access to information resources for an extended period of time. Solutions to address those eventualities should be identified in advance. Planning should address identification of responsible individuals who are authorized to make decisions in response to such events, how to prevent these events from occurring, how to inform and train affected individuals, and how to recover from such events. Also see Section 6, Continuity Planning and Disaster Recovery.

B. Campus oversight

Consistent with common practices in higher education, campuses are encouraged to form an electronic information management group composed of representatives of campus constituencies to review campus electronic information management activities and to establish a framework for an integrated data environment.

Campus Advisories for Policy on Stewardship of Electronic Information Resources

Since the academic enterprise collects and processes electronic information that may be subject to specific legal protections, e.g., protected health information, appropriate academic bodies should be included in campus planning to identify the proper stewardship of academic electronic information resources as well as to ensure broad dissemination of policy, guidelines, and procedures to the academic community.

Recommendations for the management of institutional electronic information should be based on common principles that:

- ensure confidentiality, integrity, and availability of institutional information in electronic form for shared access by the University community, subject to authorization requirements and confidentiality standards,
- clarify roles and responsibilities for appropriate authorization for release or disclosure of electronic information subject to federal and state law or regulation, or University policy,
- maximize data consistency to support integration and minimize duplication in capturing, storing, and maintaining data, and
- facilitate electronic information sharing by providing a reliable and secure technical environment for managing electronic information and improving direct access to electronic information by authorized users.

C. Classification of electronic information

Identification of the sensitivity of electronic information is necessary to determine appropriate practices to protect electronic information from unauthorized access or use and to protect the systems where that electronic information is stored or processed. As a first step, the Policy on Stewardship of Electronic Information Resources requires that unit and departmental management conduct inventories and classification of resources for which they are responsible. Inventories should include an assessment of the type of information managed by the departments in order to determine which security measures should be deployed.

- See Business and Finance Bulletin IS-2, Inventory, Classification, and Release of University Electronic Information for classification schemes.

D. Security Plan

When assessments indicate the presence of electronic information protected by law or policy, a security plan as outlined in Business and Finance Bulletin IS-3, Electronic Information Security should be developed. Generally, electronic information that is subject to federal or state law, such as student or financial data, protected health information, or social security numbers, including research data containing such information, requires the highest level of protection. In conformance to University policy, all systems that host highly protected electronic information must meet specific administrative, technical, and physical requirements. Systems may also be subject to additional operating regulations in accordance with vendor, partner, or funding agency agreements.

Campus Advisories for Policy on Stewardship of Electronic Information Resources

- See Appendix B for a chart listing suggested security measures to address common vulnerabilities and threats to electronic systems and data.

E. Release and disclosure

The California Public Records Act requires that the University disclose specified public records if they pertain to the business of the University. However, the release or disclosure of personal or other sensitive electronic information may be subject to federal and state law, University policy, or industry regulation. Statutes identify strict rules regarding consent for disclosure or release of information based on legitimate educational or medical need. The Electronic Communications Policy governs access to electronic communications that relate to the conduct of the University's business.

Departments should establish procedures to ensure that appropriate review of requests for access to information are reviewed and the appropriate authority approve requests to access or disclose information.

- See Business and Finance Bulletin RMP-2, [Records Retention and Disposition](#) for guidance regarding maintenance and retention of University administrative records.
- See Business and Finance Bulletin RMP-8, [Legal Requirements on Privacy of and Access to Information](#) for University policy implementing the California Public Records Act.
- Business and Finance Bulletin IS-2, Inventory, Classification, and Release of University Electronic Information includes guidelines for release and disclosure.
- See [Electronic Communications Policy](#), section [IV.B. Access without Consent](#).

4. Electronic Information Security

Protection of University information assets and the technology resources that support the UC enterprise is critical to the functioning of the University. University information assets are at risk from potential threats such as, malicious or criminal action, system failure, natural disasters, and even employee error. Such events could result in damage to or loss of information resources, corruption or loss of data integrity, interruption of the activities of the University, or compromise to confidentiality or privacy of members of the University community.

The University recognizes that absolute security of electronic information resources against all threats is an unrealistic expectation that would require the commitment of a prohibitively high level of resources. The University's goals for risk reduction are based, therefore, on the principle that the level and type of security should reflect an assessment of:

- the criticality of an electronic information resource to the operation of the University,
- the sensitivity of the data residing in or accessible through the electronic information resource,
- the cost of preventive measures and controls designed to detect errors, irregularities, or unrecoverable loss or vandalism of data, and

Campus Advisories for Policy on Stewardship of Electronic Information Resources

- the amount of risk that management at a campus, laboratory, or the Office of the President is willing to absorb.

A. Campus information security program

In conformance with the University of California Policy on Stewardship of Electronic Information Resources, Business and Finance Bulletin IS-3, Electronic Information Security requires that campuses implement an Information Security Program that includes:

- designation of authority for information security
- risk assessment strategies
- security controls recommendations
- incident response and notification procedures
- security awareness training and education program
- review of contracts with external partners

Campus information security programs should incorporate appropriate strategies that ensure reliability and recoverability. See Section 6, Continuity Planning and Disaster Recovery, below. Security programs shall undergo periodic evaluation of established safeguards to ensure that they adequately address operational or environmental changes or compliance with new legal requirements.

- See Business and Finance Bulletin, IS-3, Electronic Information Security for guidelines for developing an Information Security Program.

B. Minimum Standards

BFB IS-3 also requires that campuses establish minimum standards for devices connected to their networks. Such standards are intended to protect networked devices from a range of threats and vulnerabilities, such as malicious software, unauthorized access, unencrypted authentication, and known software and operating system vulnerabilities. Campuses should also identify specific software that is determined to pose serious security risks to their environments.

C. Encryption

Suitably strong encryption measures employed and implemented with appropriate assurance can reduce the risk of disclosure of electronic information to unauthorized parties. Portable devices and media (for example, laptops, PDAs, thumb drives, etc.) present major risks for unauthorized disclosure of electronic information. Appropriately deployed encryption can mitigate these risks.

- See Business and Finance Bulletin IS-3, Appendix D for encryption recommendations.

5. Identity and Access Management

Identity and access management allows for accurate identification of members of the Campus communities, allowing appropriate authorized and authenticated access to University

Campus Advisories for Policy on Stewardship of Electronic Information Resources

electronic information resources. Campus identity and access management programs may address a range of issues regarding:

- accurate identification of members of campus communities,
- accurate and timely information about campus community members
- reduction of redundant and vulnerable identity data repositories,
- protection of personal information in enterprise directories from unauthorized access or exposure,
- reduction of administrative overhead to create, update, and delete individual accounts for access to network-based services,
- authorization and authentication infrastructure, protocols, and interfaces that support secure access to online services, and
- maintenance of records that ensure auditable and legally compliant tracking of access to online services.

Campus identity and access management programs should be in conformance with University policies.

- See BFB IS-11, Identity and Access Management for University guidelines.

6. **Continuity Planning and Disaster Recovery**

Appropriate stewardship of information resources requires that departments and units collaborate with campus emergency planning and recovery efforts to ensure availability and integrity of those information resources identified as critical for the functioning of the campus, department, or unit. An assessment of the most probable risks, hazards, and losses that may occur at a particular location determines the scope of continuity planning activities.

Continuity planning includes the identification of criticality of systems and services into the following categories: essential, necessary or deferrable. Continuity planning comprises the following phases: mitigation, preparedness, response, and recovery.

- See IS-12, Continuity Planning and Disaster Recovery for the University guidelines for Continuity Planning and Disaster Recovery.

7. **Common IT Architecture**

Campuses would benefit from the development of a business architecture that “scales to meet the challenges driven by enrollment growth, technological advances, and rising expectations of constituents.”¹

A unified technical architecture will provide a framework for delivering secure services based on common operational principles that foster productivity and effectiveness of University administrative and academic processes and that enable interoperability and sharing of technology both within campuses and between campuses, medical centers, and

¹ UC 2010, A New Business Architecture for the University of California, July 2000.
<http://www.ucop.edu/irc/nba/welcome.html>

Campus Advisories for Policy on Stewardship of Electronic Information Resources

national laboratories. Increased cost reductions are realized through economies of scale in purchasing strategies that conform to the campus architecture.

Issues to be addressed within an architectural framework include:

- identification of strategic technology directions, architectural planning, and implementation of appropriate emerging technology standards,
 - guidance for campus departments to plan new information systems consistent with the campus architecture,
 - recommended application software management strategies and pursuit of opportunities in support of interoperability and common technologies,
 - establishing guidelines and standards for applications used in the conduct of University business, such as user interface, accessibility, supported platforms, and shared services,
 - establishing standards for authentication, authorization, and identity data exchange, and
 - establishing common infrastructure in conformance with architectural planning objectives that facilitate sharing among multiple applications.
- See [Part 2, Responsibility and Authority](#), in Business and Finance Bulletin [BUS-43 Materiel Management](#) for specific authorization requirements for acquisition of goods and services.

Appendix A: Related Policies and Supporting Resources

- Statement of Ethical Values and Standards of Ethical Conduct
- Electronic Communications Policy
- Safeguards, Security and Emergency Management Policy
- Academic Personnel Manual, Section 160.
- Policies Applying to Campus Activities, Organizations, and Students, [Section 130.00](#).
- Accounting Handbook
- Business and Finance Bulletins
 - BUS-43, Materiel Management
 - IS-2, Inventory, Classification, and Release of University Electronic Information
 - IS-3, Electronic Information Security
 - IS-10, Systems Development Standards
 - IS-11, Identity and Access Management
 - IS-12, Emergency Planning and Disaster Recovery
 - RMP-2, Records Retention and Disposition: Principles, Processes, and Guidelines
 - RMP-8, Legal Requirements on Privacy of and Access to Information
- Security at the University of California Website <http://www.ucop.edu/irc/itsec/uc>
Selected Links:
 - [Campus Security Program](#)
 - [Risk Assessment Resources](#)
 - [Incident Handling Overview](#)
 - [Guidelines for Restricted Resources](#)
 - [Log Management Issues and Recommendations](#)
 - [Encryption Overview and Recommendations](#)
 - [Issues to Include in Contracts](#)
- HIPAA at the University of California Website
<http://www.universityofcalifornia.edu/hipaa/welcome.html>

Appendix B Security Controls for Common Vulnerabilities/Threats

Threat/vulnerability	Risk	Security Controls
Older versions of operating systems and application software	Hackers search out Internet-connected systems on which security patches for publicized vulnerabilities have not been installed. By locating un-patched devices, hackers can exploit known vulnerabilities and obtain complete access to system and data files. Risk loss of confidentiality, integrity, and availability (data loss or damage, unauthorized acquisition of data, or inaccessible service). May require notification to impacted individuals. Risk damage to reputation and financial cost.	Timely update of operating system and application software with announced security patches.
Malicious programs such as virus, worm, Trojan horses, spyware	Loss of integrity to operating system or data; unauthorized access to systems and files. May require notification to impacted individuals. Risk to privacy, reputation; financial costs.	Install anti-virus, anti-spyware software, and firewalls.
Equipment theft or loss	Loss of data; unauthorized acquisition of data. May require notification to impacted individuals. Risk to privacy, reputation; financial cost.	Software protection (such as encryption or tamper-proof password-protected devices). Physical access controls (such as facility access management, lock-down devices, locked doors). De-identification of personal information. Timely back up of system/data.
Intrusion (unauthorized access via the Internet or "in person")	Loss of integrity to operating system or data; unauthorized access to systems and files. May require notification to impacted individuals. Risk to reputation; financial costs.	Firewalls, strong passwords. De-identification of personal data. Physical access controls, lock screen-savers.
Insecure network transmissions	Unauthorized access to transmission; unauthorized acquisition of data. May require notification to impacted individuals. Risk damage to reputation and financial cost.	VPN, SSL, https, secure FTP, secure email services.

Appendix B Security Controls for Common Vulnerabilities/Threats

Threat/vulnerability	Risk	Security Controls
Human error; intentional disruption of service	Despite all technical controls, systems or data may be subject to loss of confidentiality, integrity, and availability. May require notification to impacted individuals. Risk damage to reputation and financial cost.	Management oversight; education/training; background checks. Log management strategies that report anomalies. Deployment of software products that search out vulnerabilities in systems design, coding, etc.
Improper disposal of equipment	Unauthorized access to information on the system. May require notification to impacted individuals. Risk damage to reputation and financial cost.	Encryption; sufficient removal/cleaning of disks/files.
Social engineering and other email scams, e.g., phishing	Unwittingly provide personal information/data/passwords to unauthorized sources. Risk threat of identity theft.	Education and awareness training