

University of California
Guidelines for Stewardship of Electronic Information Resources
Draft: For Comment Only

1. Introduction

The University of California recognizes the ubiquitous use of electronic information resources for the conduct of its activities in support of teaching, research, and public services. Appropriate stewardship of these resources and the information assets they support is essential for efficient and effective functioning of University electronic information resources and to ensure the safeguarding of personal, confidential, or other sensitive electronic information.

The purpose of these Guidelines is to support the [University Policy on Stewardship of Electronic Information Resources](#). They describe the primary objectives, goals, and recommendations for safeguarding and supporting electronic information resources at the University of California. The Guidelines identify electronic information management practices that should be implemented as appropriate in all University environments. Principles of academic freedom, shared governance, privacy, and administrative efficiency establish important criteria for the management of electronic information resources. These Guidelines reflect these firmly-held principles within the context of the University's legal and other obligations.

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 personal information. The Business and Finance [Records Management and Privacy](#) bulletins identify University standards for disclosure and release of information about individuals and set forth guidelines for University records management. For guidelines governing privacy of student information, see [Policies Applying to Campus Activities, Organizations, and Students, section 130.00](#). The University of California [Academic Personnel Manual, section 160](#), describes the privacy rights of academic employees. The [Electronic Communications Policy](#) sets forth policy and procedure regarding the examination, monitoring, or disclosure of personal electronic communications records. Guidelines regarding the privacy and protection of health information are available at the [UC HIPAA website](#).

Each University department and individual in the University community plays a role in achieving excellence in the stewardship of University information assets. The University [Statement of Ethical Values and Standards of Ethical Conduct](#) articulate the University's expectation that units and individuals will be held accountable to these high standards.

2. Electronic Information Management

The proper management and use of electronic information is intended to ensure privacy protections, foster clear accountability, increase the effectiveness of data administration, and minimize legal exposure and liability associated with the improper use of electronic information stored, processed, or transmitted by University individuals or electronic information systems.

A. Campus oversight

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. 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,
- ensure clarification of 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.

The academic enterprise, whether in its instructional, research, or other scholarly endeavors, may collect and process vast quantities of electronic information subject to specific legal protections. In particular, any electronic information that may identify an individual or relate to that individual, such as social security numbers or protected health information, requires specific protection. Appropriate academic bodies should be included in campus planning to identify the proper stewardship of academic electronic information resources and to ensure broad dissemination of policy, guidelines, and procedures to the academic community.

B. Inventory and classification of electronic information

The proliferation of data in electronic information systems has resulted in high levels of vulnerability in the management of electronic information. It is essential that inventories be conducted to identify the nature of the electronic information and the systems hosting electronic information.

It may be necessary to scan devices or systems, particularly systems that host large amounts of electronic information that have been compromised by a security breach, to identify the existence of data subject to notification requirements. If such scanning is necessary, individuals who are responsible for managing electronic information should provide notice to others who may store information on the scanned system. Such scanning should be conducted in conformance with the least perusal provisions of the [Electronic Communications Policy](#). Results of scanning activities should be returned to the individuals responsible for management of the 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. For

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

Generally, electronic information that is subject to federal or state law, such as student or financial data, protected health information, or social security numbers, requires the highest level of protection. 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 or partner agreements, such as the Payment Card Industry Data Security Standards.

If an inventory reveals that electronic information protected by law and policy is processed, stored, or transmitted, individuals who manage resources supporting such information should develop a security plan as outlined in Business and Finance Bulletin IS-3, Electronic Information Security. All individuals who access protected information should receive appropriate training regarding their obligations and recommended procedures for safeguarding the information.

Systems that host electronic information identified as critical to the continuing operation of the campus or of the University must be included in disaster recovery plans. See section 5, Continuity Planning and Disaster Recovery, below.

C. 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 (see Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information). However, the release or disclosure of personal or other sensitive electronic information may be subject to federal and state law or University policy. Statutes identify strict rules regarding consent for disclosure or release of information based on legitimate educational or medical need.

In order to ensure appropriate disclosure or release of electronic information, permission for access to specific data must be granted by the University official who has been assigned overall management responsibility for the electronic information system or data managed by that system. Sharing of electronic information with UC administrative units is allowed for legitimate business needs.

Any agreements with vendors for the processing, storage, or transmission of University information must include provisions that ensure compliance with federal and state law and University policy.

See section 4, Identity and Access Management below for guidelines regarding access strategies. Also, Business and Finance Bulletin RMP-2, Records Retention and Disposition: Principles, Processes, and Guidelines offers general guidance regarding maintenance and retention of University administrative records, such as requests for access to or disclosure of public or sensitive electronic information.

To fulfill its role as the corporate headquarters of the University of California, the Office of the President must obtain specific electronic information from campus operational systems. Information Resources and Communications – UCOP supports the policy analysis, planning, and reporting needs of the University by developing and maintaining systems that collect corporate data and by enabling access to this data. Requests for data from campuses are made in support of the University's budgeting process, policy formulation, long-term planning, policy monitoring, internal reporting to the Regents and other University entities, and external reporting to state, federal, and other external agencies as required.

For more guidance on disclosure and release of electronic information, see Business and Finance Bulletin IS-2, Inventory, Classification, and Release of University Electronic Information.

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

Every individual in the University community is responsible for appropriate protection of the information resources over which he or she has jurisdiction or control. Operators of University information resources are expected to follow appropriate professional practices in providing for the security of information resources, data, application programs, and systems in their area of responsibility.

See Business and Finance Bulletin IS-3, Electronic Information Security for more detailed guidelines.

A. Campus information security program

Each campus must establish an information security program which includes:

- identification of an individual who is responsible for campus compliance with its security program,
- risk assessment strategies to identify vulnerabilities and threats for departmental information resources as well as major enterprise systems,
- recommendations for administrative, technical, and physical security measures to address identified risks relative to their sensitivity or criticality,
- incident response planning and notification procedures,
- security awareness training, education, and certification as appropriate for all University community members,
- appropriate review of third-party agreements for compliance with federal and state law and University policy.

Campus information security programs should incorporate appropriate strategies that ensure reliability and recoverability. See Section 5, 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.

B. Minimum requirements for network connectivity

Each campus must establish minimum standards for devices connected to their networks to prevent those devices from being subverted to attack other elements of the campus IT environment. Standards must address, at the least:

- **access control measures**
to allow only authorized individuals access to information resources,
- **encrypted authentication**
to protect against surreptitious monitoring of passwords,
- **system security and change-management practices**
to ensure timely update of security patches,
- **anti-virus software**
to protect every level of device as appropriate for specific operating systems,
- **removal of unnecessary services**
to prevent surreptitious use of services not needed for the intended purpose or operation of the device – such services should be turned off,
- **host-based firewall software** (as appropriate and as available)
to limit network communications to only those services required to be made accessible over the network,
- **authenticated email relay**
to prevent unauthorized third parties to relay email messages,
- **authenticated network proxy servers**
to prevent an attacker from executing malicious programs on servers by use of anonymous user accounts, and
- **re-authentication measures**
to prevent unauthorized users to access services or devices left unattended for an extended period of time.

Campuses should also identify and prohibit the use of specific software that is determined to pose serious security risks. Devices that host highly sensitive or critical information may be subject to additional requirements as noted in section 2.B, Electronic Information Management, above.

C. Encryption

Suitably strong encryption measures employed and implemented with appropriate assurance can prevent the disclosure of electronic information to unauthorized parties. Encryption of information in transit across communication systems protects information from observation during transmission. Encryption of information in storage protects information from being accessed when an unauthorized individual gains physical access to a device.

Transit

Wherever deemed appropriate, data requiring the highest level of protection should be encrypted during transmission using encryption measures strong enough to minimize the risk of the data's exposure if intercepted or misrouted.

Storage

Encryption of information in storage presents risks to the availability of that information, due to the possibility of encryption key loss. Therefore, the use of encryption must take into account the nature of the information resources and the University's requirements for the timely or continued availability of the information.

Records subject to disclosure under the California Public Records Act (see Business and Finance Bulletin RMP-8) or required to be accessible for defined periods of time in compliance with the University of California Records Disposition Schedules Manual must be available to appropriate University officials at all times. Other information that may be required to conduct the University's business must also be available when needed. Therefore, at least one copy (the *authoritative* copy) of any such information shall be stored in a known location in unencrypted form or, if encrypted, the means to decrypt it must be available to more than one person.

Portable devices

Data that requires a high level of protection (see 2.B Inventory and classification of electronic information, above) may be retained on portable devices only if protective measures, such as encryption, are implemented that safeguard the confidentiality or integrity of the data in the event of theft or loss of the portable equipment.

Key management

Campuses must implement encryption key management plans to ensure the availability of the encrypted *authoritative* copy.

- The encryption key management plan must ensure that data can be decrypted when access to data is necessary. This requires backup or other strategies to enable decryption, thereby ensuring that data can be recovered in the event of loss or unavailability of cryptographic keys.

- The encryption key management plan must address handling compromise or suspected compromise of encryption keys. A contingency plan should address what actions should be taken in the event of a compromise, such as with system software and hardware, cryptographic keys, or encrypted data.
- Users must be made aware of their unique role if they are given responsibility for maintaining control of cryptographic keys.
- Management of encryption keys and key management software and hardware must be a University employee holding a *Critical Position*¹.

More information on encryption strategies is available from Business and Finance Bulletin IS-3, Electronic Information Security.

4. Identity and Access Management

Identity and access management typically consist of the following:

- **identification**
The identity of individuals must be confirmed by their presentation of valid current primary government issued photo ID to the campus unit that manages electronic identity information and that provides identity information and authentication services for their campus.
- **registration**
The process of adding identified individuals to an enterprise directory and issuing digital credentials, e.g., NetIDs and passwords, to the individual,
- **authentication**
The act of confirming the identity of an individual by verification of digital credentials used by the individual to gain access to a network-based service,
- **authorization**
The process of ensuring that an identified individual or service, properly authenticated, is permitted to access a specific network-based service. It may also grant the identified individual permission to perform specific activities.

Reliance on electronic information resources to conduct University activities requires that campuses have in place an identity and access management strategy to address issues regarding:

- accurate identification of members of campus communities,
- enterprise directories that ensures accurate and timely information about campus community members and reduces redundant and vulnerable identity data repositories,
- protection of private information in enterprise directories from unauthorized access or exposure,
- ability for efficient and timely authorization of campus community member access to and use of network-based services as well as timely termination of access authorization,
- reduction of administrative overhead to create, update, and delete accounts for access to network-based services,

¹ The term "Critical Position" is used here as defined in University Personnel policies, and is not to be confused with the use of the term "critical" as used in these Guidelines with respect to information systems.

- availability of network-based services that provide access to information in enterprise directories,
- authorization and authentication infrastructure, protocols, and interfaces that support secure access to online services and information exchange between network-based applications, including appropriate encryption measures to protect the privacy of the digital credential used for authentication, and
- maintenance of records that ensure auditable and legally compliant tracking of access to online services.

See BFB IS-11, Identity and Access Management for University more guidelines on identity and access management.

Authorization and authentication infrastructure, protocols, and interfaces must be in compliance with BFB IS-3, Electronic Information Security.

5. Continuity Planning and Disaster Recovery

University policy requires that each campus implement a comprehensive and effective program encompassing risk assessment, risk mitigation, emergency preparedness and response, and business recovery to strengthen crisis and consequence management capabilities across the University system. Assessments of the most probable risks, hazards, and losses that may occur at a particular location should define the scope of campus programs.

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.

A. Identification of criticality

Continuity planning requires the identification of systems and services that are:

- **essential** to the continuing operation of the University, that is that failure to function correctly and on schedule could result in a major failure to perform mission-critical functions, a significant loss of funds or information, or a significant liability or other legal exposure.
- **necessary** to perform important functions, but operations could continue for a short period of time without those functions while normal operations are being restored.
- **deferrable** while operations continue for an extended period of time without those systems or services performing correctly or on schedule.

B. Continuity planning phases

Continuity planning requires that impact analyses be conducted to identify the effect of potential resource loss in the event of an emergency or disaster. Planning should also consider the impact of pandemic events that would reduce the availability of human resources or that mandate facility closures. The analysis should set forth a framework to

enable decision making throughout the emergency, and offer a roadmap for response and recovery. Planning phases should include:

- **mitigation:** the identification of steps that can be taken to reduce the potential for risks, hazards or losses;
- **preparedness:** planning should include issues, such as identification of emergency authorities, communication plans, deployment of personnel, identification of remote worksites, deployment procedures to relocate or replicate resources or facilities, and measures to protect vital records or essential data;
- **response:** identification of priorities and activities that address the immediate and short-term effects of the emergency; and
- **recovery:** steps to achieve the timely resumption of systems and services.

For additional guidelines, see IS-12, Continuity Planning and Disaster Recovery.

6. Common IT Infrastructure

The University is committed to the development of a business architecture that will “scale to meet the challenges driven by enrollment growth, technological advances, and rising expectations of constituents.”² A unified technical infrastructure 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 national laboratories. Increased cost reductions are realized through economies of scale in purchasing strategies that conform with the campus infrastructure.

Campuses are encouraged to:

- identify strategic technology directions, conduct infrastructure planning, and implement appropriate emerging technology standards,
- guide campus departments to plan new information systems consistent with the campus architecture,
- recommend application software management strategies and pursue opportunities in support of interoperability and common technologies,
- establish guidelines and standards for applications used in the conduct of University business, such as user interface, accessibility, supported platforms, and shared services, and
- establish standards for authentication, authorization, and identity data exchange.

Guidelines and standards for inter-campus interoperability should be accommodated by the campus common infrastructure.

Acquisitions of computer-related hardware, software, services, and supplies result in significant annual costs to the University. To ensure economies of scale, conformance with campus infrastructure, and compliance with licensing requirements, campuses should ensure

² UC 2010, A New Business Architecture for the University of California, July 2000.
<http://www.ucop.edu/irc/nba/welcome.html>

that purchases of technology-based high-value goods and services receive appropriate review as early in the procurement process as possible.

See Part 2, Responsibility and Authority, in BFB BUS-43 Materiel Management for specific authorization requirements for acquisition of goods and services.

7. Responsibilities

A. Systemwide

The Associate Vice-President – Information Resources and Communications, Office of the President is responsible for the Policy on Stewardship of Electronic Information Resources and these supporting Guidelines.

The Information Technology Leadership Council, whose membership is appointed by Chancellors, medical center directors, and UC managed national laboratory directors, works in partnership with the UC academic and administrative leadership to identify systemwide and common campus implementation strategies.

B. Campus

Chancellors, and for the Office of the President, the Senior Vice President, Business and Finance, are responsible for delegating responsibility for implementation of these Guidelines at their respective locations. Information Security Officers are responsible for facilitating campus compliance with the campus Information Security Program.

C. Divisions and Departments

Division deans, department chairs, and appropriate administrative officials are responsible for establishing pertinent procedures and identifying appropriate practices to achieve departmental compliance with campus implementation recommendations.

D. Individuals

All members of the University community are expected to comply with campus implementation plans and to exercise responsibility appropriate to their position and delegated authorities. Each individual is expected to conduct the business of the University in accordance with the Statement of Ethical Values and the Standards of Ethical Conduct, exercising sound judgment and serving the best interests of the University.

8. 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>