

University of California
Policy on Stewardship of Electronic Information Resources

The University of California is committed to high standards of excellence in the stewardship of its electronic information resources and endorses information technology management practices that uphold principles of academic freedom, shared governance, open access, and privacy.

This Policy establishes information technology management strategies to promote responsible practices in the management of electronic information resources¹ stored, transmitted, or processed by University electronic systems. These strategies reflect University principles and are based on criteria that ensure timely and open access to information, confidentiality, the integrity of resources, administrative efficiency, and compliance with law and University policy.

This policy addresses the following strategies:

- Oversight of Electronic Information
- Information Security Program
- Identity and Access Management
- Continuity Planning and Disaster Recovery

Oversight of Electronic Information

Appropriate management of electronic information stored, processed, or transmitted by University individuals or electronic information systems entails practices that ensure privacy protections, foster clear accountability, increase the effectiveness of data administration, and minimize legal exposure and liability. Therefore, to achieve these goals, individuals who oversee the management of electronic information resources shall follow appropriate professional information management practices. In particular, they shall adhere to the following:

- **Inventories of Electronic Information.** Inventories and classification of electronic information resources shall be conducted and updated periodically.
- **Disclosure and Release of Information.** Permission for access to information or release and/or disclosure of information shall be granted in conformance with University policy and applicable laws by the University authority that has been assigned overall management responsibility for that information.
 - Sharing of sensitive electronic information with UC administrative units is allowed for legitimate business needs. Campuses² shall provide specific electronic information to the Office of the President as required.
- **Compliance with campus Information Security Program** (see below)

University guidelines are available in Business and Finance Bulletins IS-2, Inventory, Classification, and Release of University Electronic Information

¹ The term “Electronic Information Resources” applies to electronic resources as defined in Business and Finance Bulletin IS-3, Electronic Information Security.

² The term “campus” is used throughout this Policy in reference to all University locations.

Information Security Program

The management of University electronic information resources shall provide for the security of information systems, data, and application programs. In compliance with Business and Finance Bulletin IS-3, Electronic Information Security, each campus shall establish an Information Security Program that includes the following elements:

- Information Security Officer(s)
- Risk Assessments
- Security Controls
- Incident Response and Notification
- Training
- Contract Review

Identity and Access Management

Many University electronic information resources are openly available without authorization. However, access to certain resources should be granted to specific individuals only upon appropriate identification and authorization. Campuses shall implement appropriate identity and access management programs that

- accurately identify members of their campus communities,
- provide secure authorization and authentication access to sensitive information resources, and
- ensure timely granting and revocation of access privileges.

See Business and Finance Bulletin IS-11, Identity and Access Management for University guidelines.

Continuity Planning and Disaster Recovery

University policy requires that each campus implement a comprehensive and effective program that encompasses risk assessment, risk mitigation, emergency preparedness and response, and business recovery to enable and strengthen University capabilities for crisis and consequence management.

- Unit and departmental management shall collaborate with campus emergency planning and recovery coordinators to ensure the availability and integrity of critical information resources.
- Systems that host electronic information identified as critical to the continuing operation of the campus or the University shall be included in disaster recovery plans.

See Business and Finance Bulletin IS-12, Emergency Planning and Disaster Recovery for University guidelines.

Authority and Responsibilities

University campuses and medical centers, the Office of the President, and the UC managed national laboratories are responsible for implementing this policy and establishing supporting procedures and training programs as needed.

Further, in accordance with the [Statement of Ethical Values and Standards of Ethical Conduct](#), members of the University community will be held accountable for compliance with applicable laws and University policies and directives.

- **Systemwide**

This Policy is issued by the President of the University of California. The Associate Vice President – Information Resources and Communications is responsible for interpretation of this Policy and referenced Business and Finance Bulletins.

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.

- **Campus**

Chancellors, the Executive Vice President – Business Operations at the Office of the President, and UC managed national laboratory directors are responsible for delegating responsibility for implementation of this Policy at their respective locations and for ensuring that individuals are held accountable for fulfilling their responsibilities for the stewardship of electronic information resources. Information Security Officers are responsible for facilitating campus compliance with its Information Security Program.

- **Divisions and Departments**

Division deans, department chairs, and appropriate administrative officials are responsible for identifying and establishing procedures to achieve departmental compliance with the campus implementation of this Policy.

- **Individuals**

All members of the University community are expected to comply with the campus policies and procedures in support of this Policy and to exercise responsibility appropriate to their position and delegated authorities. Each member of the University community is responsible for appropriate protection of the electronic information resources over which he or she has jurisdiction or control.

Additional University Resources

- Business and Finance Bulletins in the [Information Systems](#) (IS) series offer detailed guidance about recommended information technology practices.
- Business and Finance Bulletins in the [Records Management and Privacy](#) (RMP) series provide guidance regarding University records management, public records procedures, and handling of personal information.
- [Electronic Communications Policy](#) offers guidance with respect to electronic communications.
- [Campus Advisories for Policy on Stewardship of Electronic Information Resources](#) includes references to related University policies, guidelines, and practices and provides additional recommended stewardship practices.

Definitions

- See [Glossary of Terms](#) for definitions of commonly used terms.