

IS-2 Inventory, Classification, and Release of University Electronic Information



Refer questions to Information Resources and Communications
University of California Office of the President

Revised
October 17, 2006

DRAFT FOR COMMENT ONLY

Table of Contents

I. Purpose and Scope	2
II. Definitions.....	2
III. Inventory and Classification of Electronic Information Resources	3
A. Security Objectives.....	3
1. Confidentiality.....	3
2. Integrity	6
3. Availability	6
B. Security Impact	7
C. Determination of security measures	7
IV. Guidelines for Release and Disclosure	8
A. Ownership	8
B. Release and disclosure.....	9
1. Public Information.....	9
2. Student Educational Records	9
3. Academic Personnel Records.....	9
4. Electronic Communications Records	9
C. Roles and Responsibilities: Proprietors and Custodians	10
1. Resource Proprietors	10
2. Resource Custodians	10
V. Major Responsibilities	11
A. Systemwide.....	11
B. Campus	11
C. Divisions and Departments.....	11
D. Individuals	11
VI. References.....	11
Appendix A - Definitions.....	13

I. Purpose and Scope

The University of California Policy on Stewardship of Electronic Information Resources endorses a high standard for appropriate management of University information assets and the technology resources that support the UC enterprise. The University electronically processes, stores, and transmits an enormous range of tangible information – academic and business data: intellectual works, data stores, research results – that are subject to potential damage or compromise to the confidentiality or privacy of this information unless appropriate preventative strategies are implemented.

The Stewardship Policy and its supporting Guidelines outline the obligations of University campuses, medical centers, national laboratories, and the Office of the President regarding management of these information assets.

The purpose of this bulletin is to provide further guidance for assessing the importance of information assets:

- to aid risk assessments in conformance with University IT security policy and
- to identify the need for specific security measures to ensure the appropriate level of protection for resources.

This bulletin also references existing University policy regarding the access to, release, or disclosure of University information.

All faculty, staff, students, contractors, authorized affiliates, guests, and visiting scholars are responsible for conformance with these guidelines as appropriate to their roles.

II. Definitions

The following terms used in these Guidelines are defined in Appendix A.

Authorized Individual
Confidential Information
Electronic Information Resource (Resource)
Nonrepudiation
Public Information
Resource Custodian
Resource Proprietor
Restricted Information

III. Inventory and Classification of Electronic Information Resources

University IT security policy requires that appropriate risk assessments be conducted

- to inventory and determine the nature of electronic information assets held or managed by the department and
- to understand and document the impacts in the event of failures that may cause loss of confidentiality, integrity, or availability.

See section III.B, Risk Assessment in Business and Finance Bulletin IS-3, Electronic Information Security.

A. Security Objectives

Confidentiality, integrity and availability are the three primary security objectives cited in federal legislation mandating IT security. The Federal Information Security Management Act of 2002 (FISMA)¹ defines “information security” to mean:

“Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide:

- **confidentiality**, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information,
- **integrity**, which means guarding against improper information modification or destruction, and may include ensuring information and authenticity,
- **availability**, which means ensuring timely and reliable access to and use of information.”

1. Confidentiality

The confidentiality of electronic information assets, and therefore the level of security required, depends in part on the sensitivity of the information retained on or accessible through electronic information resources.

a. Confidential Information

The term *confidential information* applies broadly to information for which access or disclosure may be assigned some degree of sensitivity, and therefore, for which some degree of protection or restricted access may be identified. Unauthorized access to or disclosure of information in this category could seriously or adversely affect the University and cause financial loss, loss of confidence or public standing, or adversely affect a partner, e.g., a business or agency working with the University.

¹ See FISMA, 44.U.S.C., Sec. 3542.

State and federal agencies may explicitly define the term “confidential” in agreements or contracts. For example, the California State Administrative Manual defines confidential information as “information maintained by state agencies that is exempt from disclosure under the provisions of the California Public Records Act.” Use of such data by University researchers requires appropriate security plans when confidential information is transferred from state agencies to the University.

Contracts and agreements may use the term “confidential” information when stating restrictions or other requirements for protection, access to, or disclosure of information governed by the agreements. Information in this category may have limited, moderate, or severe impact on University functions, which must be determined through risk assessment or business impact analysis.

b. Personal and public information

Federal and California law and University policy require protection for information that *personally identifies* or *describes* an individual and establishes requirements for any disclosure or release of personally identifiable information. Loss, corruption, or unauthorized access to personal information could result in a serious adverse effect, with widespread impact on individual privacy.

- Business and Finance Bulletin [RMP-8, Legal Requirements on Privacy of and Access to Information](#), provide guidelines for University compliance with the State of California Information Practices Act of 1977 (IPA), which guarantees certain legal rights to privacy by establishing strict limits to access to Information about an individual which is maintained by a public entity, whether that access is by a governmental agency, a private corporation, a member of the public, or an employee of the same public entity.
- The California Public Records Act requires that the University disclose specified public records if they pertain to the business of the University. Public information that is not exempt from disclosure under the provisions of the California Public Record Act is defined in RMP-8. Any disclosure of public records must be conducted according to procedures identified in RMP-8.
- [Section 160](#) of the [Academic Personnel Manual](#) recognizes the importance of the right of privacy for faculty personnel reviews and the right to privacy for evaluations and letters of recommendation. Section 160-20 (b) (5) defines personal information as it pertains to faculty. Section 160-20 (b) also defines “non-personal” “confidential” and “non-confidential” information.

- [University Policies Applying to Campus Activities, Organizations, and Students](#) provide guidelines for UC compliance with the Federal Family Educational Rights and Privacy Act (FERPA). [Section 130.00 Policies Applying to the Disclosure of Information from Student Records](#) defines “personally identifiable information” and “directory [public] information” as these terms pertain to students.
- Personal information regarding an individual’s health is subject to the Federal Health Insurance Portability and Accountability Act of 1996. University compliance guidelines are posted on the University website: [HIPAA Compliance at the University of California](#)
- Personal information associated with any loan activity is subject to the Financial Services Modernization Act of 1999; University compliance can be found in the University of California [Information Security Program](#).
- Other personal information may be considered personally identifiable information if there is a reasonable basis to believe that the information can be used to identify the individual.
- Protection of personal information may also be subject to additional operating regulations in accordance with vendor or partner agreements, such as the Payment Card Industry Data Security Standards.

c. Restricted Information

The term *restricted information* describes any confidential or personal information which is **protected by law or policy** as referenced above and that requires the highest level of security protection, whether in storage or in transit.

Section 1798.29 of the California Civil Code, which enacts the security breach notification requirement of the IPA, defines the specific personal information that is subject to that section of the IPA. This “notice-triggering information” (name plus Social Security Number, driver’s license or California identification card number, or financial account number with a security code) should be classified as restricted information. Section III. D in BFB IS-3, Electronic Information Security includes guidelines for University compliance.

The term *restricted* should not be confused with that used by the University-managed national laboratories where federal programs may employ a different classification scheme.

See IS-3, Electronic Information Security, Appendix B for a list of the security measures mandated for restricted information.

2. Integrity

The impact of unauthorized destruction or modification of an information asset must be analyzed in the risk assessment to guide determination of security measures. The HIPAA security rule specifically requires the protection of health information from improper alteration or destruction and the implementation of mechanisms to ensure that electronic protected health information has not been altered or destroyed in an unauthorized manner. Other integrity considerations regard defacement of websites, protection against fraud or forgery, protection of the integrity of research results, and the authenticity of communications (nonrepudiation).

Recommended security measures should be determined as a result of the analysis of

- purpose of an information resource and
- potential harmful impact if integrity of that resource is damaged.

Risk assessment should determine the level of importance of retaining the integrity of the information.

The analysis should include consideration of both transmission and storage of the information.

3. Availability

An assessment of the availability of information resources should take into consideration its importance for the function of the University program or information resource itself and the importance for availability to either the public or to University community.

An analysis of availability should take into account the *criticality* and priority status of the information resource. The Guidelines for Stewardship of Electronic Information Resources classify criticality as:

- **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.

Information resources classified as essential must be included in disaster recovery planning. See IS-12, Emergency planning and Disaster Recovery for further guidance.

B. Security Impact

Risk assessments should consider impact of the potential harm that failure to achieve any of these security objectives would have on University operations, functions, image or reputation, assets, or the privacy of individual members of the University community.

A framework for categorizing impact into three potential levels of risk is offered by federal standards.²

- **low:** the event could be expected to have a *limited* adverse effect or cause a negative outcome, or result in *limited* damage to operations or assets, requiring *minor* corrective actions or repairs
- **moderate:** the event could be expected to have a *serious* adverse effect or cause a significant degradation in mission capability, place the organization at a significant disadvantage, or result in *major* damage to assets, requiring *extensive* corrective actions or repairs
- **high:** the event could be expected to have a *severe* or *catastrophic* effect on operations, assets, or individuals and could be expected to cause a loss of mission capability for a period that poses a threat to human life, results in a loss of major assets, or would result in significant financial or reputational impact.

C. Determination of security measures

An analysis of Security Objectives (confidentiality, integrity, availability) and the Security Impact (low, moderate, high) for information assets, in the context of the operational goals of the unit, shall determine which security measures should be implemented. For example, information assets with a low level of confidentiality but a high degree of integrity and availability will require security measures that will ensure protection of the resource and its availability, but may not require access control measures. Some assets with a high degree of confidentiality may not require the same level of availability. Selected security measures for resources will differ depending on the outcome of the risk assessment.

The following examples suggest possible classification categorizations. The levels of risk suggested for these situations should not be viewed as a UC mandate; determination of level of risk should be based on results of individual risk assessments or impact analyses. Note that California Public Records Act or federal Freedom of Information Act requests may require disclosure or release of information in any of the categories below.

² See NIST 800-63, Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories, and FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

- **Examples:** general public unit websites, public directory information, news, campus maps
confidentiality: public information
integrity: moderate or high importance
availability: deferrable, necessary or essential
- **Examples:** internal communications, financial spreadsheets, minutes of non-confidential meetings, subsets or aggregates of data that do not expose protected personal or financial information
confidentiality: some confidentiality
integrity: moderate or high importance
availability: deferrable or necessary
- **Examples:** private communications, employee or student IDs, research data or results that do not expose intellectual property concerns, contractual information, certain management information, network transaction logs
confidentiality: some confidentiality
integrity: moderate or high importance
availability: deferrable, necessary or essential
- **Examples:** student, medical, or other large repositories of personal information, security logs, encryption keys, passwords to Resources with a high confidentiality, integrity, or availability classification, or unique identifying numbers (large repositories of credit card numbers, SSNs, financial account numbers in combination with security or access codes or passwords)
confidentiality: restricted
integrity: high importance
availability: necessary or essential

Consult IS-3, Electronic Information Security for guidance in identifying appropriate security strategies.

IV. Guidelines for Release and Disclosure

A. Ownership

All University administrative records are owned by The Regents of the University of California, and the University Records Management Program sets forth guidance for the appropriate management, disposition, and preservation of University administrative records (see [RMP-1, University Records Management Program](#)).

The University [Policy on Copyright Ownership](#) addresses ownership for works produced at, by, or through the University. The [Policy on Ownership of Course Materials](#) supplements the Policy on Copyright Ownership by clarifying existing policy concepts and extending their application to works prepared for teaching. It also provides useful guidance for faculty, staff and administrators about intellectual property rights for teaching materials in digital form.

B. Release and disclosure

Several University policies and guidelines identify obligations regarding the release, disclosure, access to, or use of information processed, stored or transmitted by University electronic information resources. See Business and Finance Bulletin [RMP-8 Legal Requirements on Privacy of and Access to Information](#) for complete University guidelines.

1. Public Information

University records pertaining to the administrative business of the University are considered public records (see Appendix A, Definitions). Other records, although not owned by The Regents, nevertheless may be subject to disclosure as public records under the California Public Records Act if they pertain to the business of the University.

2. Student Educational Records

Section [130.70 disclosure of personally identifiable information from student records to persons other than the student to whom the information pertains](#) of the University Policies Applying to Campus Activities, Organizations, and Students provides specific guidelines regarding:

- directory information (section 130.710)
- permissible disclosures of personally identifiable information (section 130.721)
- redisclosures of personally identifiable information (section 130.722), and
- requests to forward academic records (section 130.723).

3. Academic Personnel Records

Detailed guidelines regarding access to academic personnel records are expressed in [section 160](#) of the Academic Personnel Manual. In particular, see:

- section 160-20.c for access by the individual,
- section 160-20.d for access by third parties to confidential and personal information, and
- section 160-20.e for access to non-personal information.

4. Electronic Communications Records

The University [Electronic Communications Policy](#) (ECP) respects the privacy of electronic communications records and does not examine or disclose those records without consent of the holder, that is, the individual

who is in possession or receipt of electronic communications. Exceptions to access individuals' electronic communications without their consent must follow specific procedural guidelines for authorization. See Section III.A. Access without Consent in ECP [Attachment 2. Implementation Guidelines](#).

C. Roles and Responsibilities: Proprietors and Custodians

1. Resource Proprietors

If not owned by the individual who creates the information, such as the owner of intellectual property, resource proprietors are those individuals responsible for information resources and processes supporting University functions. Resource Proprietors are responsible for

- ensuring the inventory and classification of information for which they have responsibility,
- in consultation with the Resource Custodian, determining the level of risk and appropriate security strategies to address that risk,
- approving requests for access, release, and disclosure of information, and
- ensuring appropriate security awareness training for individuals they authorize to access information.

Resource Proprietors should establish and review procedures to ensure compliance with federal or state regulation or University policy.

Resource Proprietors are responsible for ensuring that University Resources are used in ways consistent with the mission of the University as a whole. The Resource Proprietor must ensure that recipients of confidential data are informed that appropriate security measures must be in place **before** *restricted* data is transferred to the destination system.

2. Resource Custodians

Resource custodians are the individuals or departments who have been delegated physical or logical control over information resources, and in that capacity, have responsibility for electronic applications, system or database administration, and any other management, support function, or training related to the electronic resource.

Resource Custodians must direct any requests for access, use, release, or disclosure of electronic information to the appropriate Resource Proprietor or owner for approval. Release of information to a third party must ensure appropriate transmission security to protect the information in transit. They must also ensure that the recipient has been fully informed that security measures on the destination system must be commensurate with physical and logical security measures on the originating system. See section III.C. 2 in IS-3, Electronic Information Security.

V. Major Responsibilities

A. *Systemwide*

The Associate Vice-President – Information Resources and Communications, Office of the President is responsible for this Bulletin.

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 Executive Vice President - Business Operations, are responsible for delegating responsibility for implementation of the guidelines and requirements in this Bulletin. 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 recommendations 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.

VI. References

Policy on Stewardship of Electronic Information Resources
Guidelines for Stewardship of Electronic Information Resources

[Academic Personnel Manual, Section 160](#)

[Policy on Copyright Ownership](#)

[Policy on Ownership of Course Materials](#)

[University Policies Applying to Campus Activities, Organizations, and Students](#)

- [Policies Applying to the Disclosure of Information from Student Records](#)
- [HIPAA Compliance at the University of California](#)

[Electronic Communications Policy](#)

- ECP [Attachment 2. Implementation Guidelines](#)

[University of California Information Security Program](#)

IS-3 Electronic Information Security

IS-12 Emergency Planning and Disaster Recovery

[RMP-1, University Records Management Program](#)

[RMP-8, Legal Requirements on Privacy of and Access to Information,](#)

Appendix A - Definitions

Authorized Individual

A University employee, student, contractor, or other individual affiliated with the University who has been granted authorization by the Resource Proprietor, or his or her designee, to access a Resource and who invokes or accesses a Resource for the purpose of performing his or her job duties or other functions directly related to his or her affiliation with the University. The authorization granted is for a specific level of access to the Resource as designated by the Resource Proprietor, unless otherwise defined by University policy.

Confidential Information

The term confidential information applies broadly to information for which disclosure or access may be assigned some degree of restriction, and therefore, for which some degree of protection or restricted access may be identified. Unauthorized access to or disclosure of information in this category could seriously or adversely affect the University and cause financial loss, loss of confidence or public standing, or adversely affect a partner, e.g., a business or agency working with the University. Information in this category may have limited, moderate, or severe impact on University functions, which must be determined through risk assessment or business impact analysis.

Electronic Information Resources (Resource)

A resource used in support of University activities that involves the electronic storage, processing or transmitting of data, as well as the data itself. Electronic Information Resources include application systems, operating systems, tools, communications systems, data – in raw, summary, and interpreted form – and associated computer server, desktop (workstation), portable devices (laptops, PDAs) or media (CD ROM, memory sticks, flash drives), communications and other hardware used to conduct activities in support of the University's mission. These resources may also be called "information assets."

Nonrepudiation

Nonrepudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Nonrepudiation is a way to guarantee that the sender of a message cannot later deny having sent the message and that the recipient cannot deny having received the message.

Public Information

Public information is any information relating to the conduct of the public's business. See [RMP-8 Legal Requirements on Privacy of and Access to Information](#). In the case of personal information the term relates to information that has been determined not to constitute an unwarranted invasion of privacy if publicly disclosed.

Resource Custodian

The authorized University personnel who have physical or logical control over the Electronic Information Resource. This includes, for example, central campus information technology departments with maintenance responsibility for an application; departmental system administrators of a local area network; and database administrators for campus-wide or departmental databases. This role provides a service to the Resource Proprietor.

Resource Proprietor

The individual designated responsibility for the information and the processes supporting the University function. Resource Proprietors are responsible for ensuring compliance with federal or state statutory regulation or University policy regarding the release of information according to procedures established by the University, the campus, or the department, as applicable to the situation. Responsibilities of Resource Proprietors may include, for example: specifying the uses for a departmentally-owned server; establishing the functional requirements during development of a new application or maintenance to an existing application; and determining which individuals may have access to an application or to data accessible via an application. All Electronic Information Resources are University resources, and Resource Proprietors are responsible for ensuring that these Resources are used in ways consistent with the mission of the University as a whole.

Restricted Information

Restricted information describes any confidential or personal information which is protected by law or policy and that requires the highest level of access control and security protection, whether in storage or in transit. The term should not be confused with that used by the University-managed national laboratories where federal programs may employ a different classification scheme.