

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
December 10, 2008

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	4
2. Integrity	6
3. Availability	7
B. Security Impact	7
C. Determination of security measures	8
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. Staff Personnel Records	10
5. Personal Information	10
6. Electronic Protected Health Information (ePHI)	10
7. Electronic Communications Records	10
C. Roles and Responsibilities: Proprietors and Custodians	10
1. Resource Proprietors	10
2. Resource Custodians	11
V. Major Responsibilities	11
A. Systemwide	11
B. Campus	11
C. Divisions and Departments	11
D. Individuals	12
VI. References	12
Appendix A - Definitions	13
Appendix B – Confidential Security Information	15

I. Purpose and Scope

The University of California is committed to high standards of excellence in the management of University information assets and the technology resources that support the UC enterprise. The University processes, stores, and transmits an immense quantity of electronic information to conduct its academic and business functions. Without the appropriate management practices, these assets are subject to potential damage or compromise to confidentiality or privacy, and the activities of the University are subject to interruption. A first step in good management involves determining what type of information the managing unit holds in order to determine and implement appropriate security controls and procedures.

The purpose of this bulletin is to establish guidelines for the classification 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 access to, release, or disclosure of University information. Roles and responsibilities at all levels in the University of California system are identified.

The provisions in this bulletin apply to all University campuses and medical centers, the Office of the President, UC-managed national laboratories, and other University locations (**campuses**¹) regarding management of its information assets. Certain UC entities, such as UC managed laboratories or medical centers, may be subject to additional federal or state law or other regulations.

All academic and staff employees, students, and other Authorized Individuals are responsible for adhering to the guidelines and requirements in this bulletin as appropriate to their roles.

II. Definitions

The following terms used in this bulletin are defined in Appendix A.

Authorized Individual
Confidential Information
Electronic Information Resource (Resource)
Non-repudiation
Public Information
Resource Custodian
Resource Proprietor
Restricted Information

¹ The term "campus" is used throughout this bulletin in reference to all University locations.

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 University units and
- to understand and document the impacts in the event of failures that may cause loss of confidentiality, integrity, or availability to those assets, and
- to identify the level of security necessary for the protection of the resources.

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 law regarding IT security. The Federal Information Security Management Act of 2002 (FISMA)² defines “information security” to mean:

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

- **Confidentiality:** preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. The assigned level of confidentiality is used in determining the types of security measures required for its protection from unauthorized access or disclosure.
- **Integrity:** guarding against improper information modification or destruction, and may include ensuring information and authenticity. The level of impact of unauthorized modification or destruction of information resources describes the importance for maintaining the integrity of a Resource.
- **Availability:** ensuring timely and reliable access to and use of information. The overall importance of availability of a Resource is based on its criticality to the functional operation of a Campus or department or to the priority of that function in continuity plans and disaster recovery strategies. Emergency management planning must take into account the availability requirements of a particular Resource to determine its inclusion in emergency and disaster recovery planning.

² See FISMA, 44.U.S.C., Sec. 3542.

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 access restriction may be warranted. Unauthorized access to or disclosure of information in this category could result in a serious adverse effect, cause financial loss, cause damage to the University's reputation and loss of confidence or public standing, or adversely affect a partner, e.g., a business or agency working with the University.

State and federal agencies or business partners 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.

Information regarding the implementation or documentation of specific security measures should be treated as confidential information. Such information could provide a roadmap for malicious attacks to University applications, systems, and networks. Increased vulnerability or risk to the University could result if such information were disclosed to unauthorized individuals. For more information see Appendix B – Confidential Security Information.³

³ When information relating directly to the security of systems is documented, it should be identified as such with the label "Confidential: Computer Security Sensitive Information". This flags material for careful examination by University attorneys when a Public Records Act request is submitted. It also makes it clear to anyone else seeing such information that extra consideration should be taken before providing access or disclosure to others.

b. Personal and public information

Federal and state law and University policy require protection of information that *personally identifies* or *describes* an individual. These laws and policies establish certain requirements for disclosure or release of personally identifiable information and for information or records defined as public information. Loss, corruption, or unauthorized access to personal information could result in a serious adverse effect, with widespread impact on individual privacy.

University policies and guidelines pertaining to personal and public information include:

- The California Public Records Act requires that the University disclose specified public records if they pertain to the business of the University. Any disclosure of public records must be conducted according to procedures identified in Business and Finance Bulletin [RMP-8, Legal Requirements on Privacy of and Access to Information](#).
- RMP-8 also provides 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 on 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.
- 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, financial account number with a security code, medical information or health insurance information) should be classified as restricted information (see Restricted Information, below).
- [Section 160](#) of the [Academic Personnel Manual](#) recognizes the importance of the right to 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.
- [PPSM 80. Staff Personnel Records](#) in the [University Personnel Policy for Staff Members](#) identifies rules governing employee personnel records.
- [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 also 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 financial 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 that is **protected by law or policy** such as those referenced above and that requires the highest level of security protection, whether in storage or in transit.

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 [BFB IS-3, Electronic Information Security](#), Appendix B for a list of the security measures for protecting restricted information. Section III. D in IS-3 includes guidelines for University notification requirements in the event of a security breach involving restricted information.

2. Integrity

The impact of unauthorized destruction or modification of an information asset must be analyzed in a risk assessment to guide determination of appropriate security measures. For example, 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 protection against fraud or forgery, protection of the integrity of

research results, defacement of websites, and the authenticity of communications (non-repudiation).

Recommended security measures should be determined as a result of an analysis of:

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

Risk assessment should determine the level of importance of maintaining 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 requirements for information resources should take into consideration their importance for the function of the University program and the importance for its availability to either the public or to the University community.

An analysis of availability should take into account the *criticality* and priority status of the information resource. [IS-12, Emergency planning and Disaster Recovery](#) defines three levels of criticality as:

- **Essential** to the continuing operation of the University. 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.

See Section C, Determination of Security Measures (below) for more information.

B. Security Impact

Risk assessments should consider the impact of 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:⁴

- **low:** The event could be expected to have a *limited* adverse effect or negative outcome to the University, or result in *limited* damage to University operations or assets, requiring *minor* corrective actions or repairs.
- **moderate:** The event could be expected to have a *significant* adverse effect on the University or cause a significant degradation in its mission capability, place the University at a significant disadvantage, or result in *major* damage to University assets, or reputation requiring *extensive* corrective actions or repairs.
- **high:** The event could be expected to have a *severe* or *catastrophic* effect on University 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 severe financial impact or impact to the reputation of the University.

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 requiring a high degree of integrity and availability will require security measures that will ensure protection of the resource and its availability, but may require different levels of 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.

Campuses should make local recommendations based on risk assessments or impact analyses as appropriate to their circumstances. Note that California Public Records Act or federal Freedom of Information Act requests may require disclosure or release of information in any categories.

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

⁴ 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.

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. These include:

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. See Business and Finance Bulletin [RMP-8 Legal Requirements on Privacy of and Access to Information](#) for University guidelines on access to public records.

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 can be found 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. Staff Personnel Records

Access to an employee's personnel record by the employee and by the public is identified in Personnel Policies for Staff Members: [80. Staff Personnel Records](#).

5. Personal Information

See Business and Finance Bulletin [RMP-8 Legal Requirements on Privacy of and Access to Information](#) for University guidelines on disclosure and release of personal information.

6. Electronic Protected Health Information (ePHI)

See [University of California Implementation of HIPAA Privacy Rule](#) for University guidelines for disclosure and release of ePHI.

7. Electronic Communications Records

The University [Electronic Communications Policy](#) (ECP) establishes requirements for access to electronic communications records and does not permit release or disclosure of those records without consent of the holder, i.e., the individual who is in possession or receipt of those records. Exceptions to access individuals' electronic communications without their consent must follow specific procedural guidelines for authorization. See Section III.A, Access without Consent in the ECP [Attachment 2. Implementation Guidelines](#).

C. Roles and Responsibilities: Proprietors and Custodians

1. Resource Proprietors

Resource proprietors are those individuals responsible for information resources and processes supporting University functions. This includes individuals who create the information, such as the owner of intellectual property. 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 ensuring implementation of appropriate security controls 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 regulations 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 should ensure that recipients of

restricted information are informed that appropriate security measures must be in place **before** *restricted* information 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. Resource Custodians must ensure that appropriate transmission security is used when releasing any information to a third party to protect the information in transit. They should also ensure that the recipient affirms that security measures on the destination system are 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 members are appointed by Chancellors, medical center directors, and UC managed national laboratory directors, works in partnership with UC academic and administrative leadership to identify systemwide and common campus implementation strategies.

B. 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 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 identifying and establishing procedures to achieve departmental compliance with campus implementation.

D. Individuals

All members of the University community are expected to comply with campus policies and procedures in support of this bulletin 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 [Standards of Ethical Conduct](#), exercising sound judgment and serving the best interests of the University.

VI. References

[Statement of Ethical Values and Standards of Ethical Conduct](#)

[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](#)

[Personnel Policy for Staff Members,](#)

[PPSM 80. Staff Personnel Records](#)

[Management Guide for Information Security](#)

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 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, damage to the University's reputation, 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), other electronic files, 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 are valued information assets of the University.

Non-repudiation

Non-repudiation means to ensure that a transferred message has been sent and received by the parties claiming to have sent and received the message. Non-repudiation 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 law or 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 that 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 “restricted” should not be confused with that used by the UC managed national laboratories where federal programs may employ a different classification scheme.

Appendix B – Confidential Security Information

Information descriptive of the specific security measures that safeguard restricted (confidential or personal) information resources represents a special class of information that should be protected from unauthorized access or disclosure. Such information – whether hardware configurations, management controls or security practices, or procedures employed – could provide a roadmap for malicious individuals to attack University applications, systems, and networks.

Examples of specific security measures:

- Documentation of known or potential vulnerabilities and risks
- Results of security scans and assessments
- Implementation/configuration details for security devices and tools
- Firewall and intrusion detection system logs
- Private credentials used to authenticate users, processes, and systems
- Security incident documentation
- Permission attributes identifying the resources to which an individual has access

Only truly sensitive security information should be so classified. General security information should not be considered confidential. For example information that is:

- generic in nature (e.g., "we operate a firewall")
- confirmation of a generally expected, common practice (e.g., "an IDS is in place")
- easily obtainable by a moderately skilled attacker (e.g., software version information obtained by scanning; reverse DNS information)
- easily/quickly guessed or tested (e.g., is port 135 open or not?)
- is a logical consequence of other IT and/or security policies

Information regarding confidential security measures may be in the form of documentation, diagrams, metadata, data, program source code, executable program code, firmware, etc., whether encrypted or not, and whether in electronic or hardcopy form.