BFB-IS-11: Identity and Access Management

Responsible Officer:	VP - Chief Information Officer
Responsible Office:	IT - Information Technology Services
Issuance Date:	7/27/2007
Effective Date:	7/27/2007
Scope:	[Scope]

Contact:	Stephen Lau
Email:	Stephen.lau@ucop.edu
Phone #:	(510) 987-0409

I.   POLICY SUMMARY

Access to and use of University electronic information resources must be performed in a manner that ensures the confidentiality, integrity, and availability, of University resources and such actions must be conducted in full compliance with federal and state law and University policies. Although many University electronic information resources are openly available without authorization, access to certain resources may only be granted to individuals who have been authorized to have such access (Authorized Individuals), and such access may be granted only upon appropriate identification and authorization. Technical and/or physical access controls should be employed to ensure conformance with University security policy and standards.

The purpose of this bulletin is to establish guidelines for identity and access management at the University of California. Identity and access management is a relatively new area for the University, so this document serves as both an educational resource and a set of guidelines for campuses in their implementation of identity and access management strategies.

Access to Resources that have been determined to be *restricted* may have more restrictive access control requirements. See IS-2, Inventory, Classification, and

[Release of University Electronic Information](#) for guidelines regarding classification of *restricted* Resources. See [IS-3, Electronic Information Security](#), section III.C.2, Operational and Technical Controls, for access control guidelines.

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) 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.

Additionally, all academic and staff employees, students, and other Authorized Individuals are responsible for conformance with these guidelines as appropriate to their roles.

II.   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.

Campus
The term "campus" is used throughout this policy in reference to all University locations.

Credential Providers
Credential Providers are the campus authorities responsible for the management of electronic identity information and for providing identity information and authentication services for their campus locations.

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.

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.

Resource Providers
Resource Providers are the organizational units with operational responsibility to provide and manage electronic information services used to conduct University business by Authorized Individuals, such as financial or student information systems. These resources are generally network-based, but may not necessarily be so.

Restricted Information
The term *restricted information* describes any confidential or personal information that is protected by law or policy 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.

III.   POLICY TEXT

Identity management describes the integration of workflow, process, and technology that enables the tracking of individual community members throughout their affiliation with the University. Identity and access management (IAM) employs critical security-based technology components and processes that simultaneously utilize centralized management of information about community members and automate processes that

enable reliable authorized access to services and resources while protecting confidential information from unauthorized access. A carefully constructed IAM system enables the University to effectively achieve its security objectives and auditable compliance with regulations regarding authorized access.

Identity and access management is based on a set of principles and control objectives to:

- ensure unique identification of members of the University community and assignment of access privileges,
- allow access to Resources only by Authorized Individuals,
- ensure periodic review of membership in the community and review of their authorized access rights,
- maintain effective access mechanisms through evolving technologies.

Secure and compliant operations rely on a well-managed IAM system that protects online resources and privacy while enabling ease of use. A successful campus identity and access management should answer questions such as:

- Are the individuals using electronic resources who they claim to be?
- Are they members of the campus community?
- Have they been granted appropriate permissions to access these resources?
- Is their personal information adequately protected?
- Do their authentication credentials meet established security standards?

Identity and access management applies a set of business rules to this total view of community to make decisions about identity and rights of access for each member of the community.

Identity Management Concepts and Core Functions
IAM systems typically include the following functions.

A. Identification

Identification is the process by which information about an individual is obtained to enable unique identification of the individual. The nature and reliability of the identification process supports some level of assurance that individuals are who they claim to be. Generally, this identity verification takes place within the office, e.g., Human Resources or Student Services, that first encounters the individual and creates their record within the institutional system(s) of record.

B. Registration and Credentialing

Registration describes the binding of the electronic credentials to data maintained about the individual in a repository that supports the authentication process (see IV.F. Enterprise Directory Services). Credentialing is the process whereby an individual is issued electronic credentials (identifier and authentication credential) for the individual's use to access Resources.

C. Authentication

Authentication is the act of confirming the unique identity of an individual by verification of the electronic credentials presented by the individual when accessing a Resource. An *authentication credential* may be:

- something the individual knows, such as a password, passphrase, or other secret information,
- something the individual has, such as a smart card with a public-key certificate,
- something that is biologically part of the individual, such as a fingerprint or a retina.

D. Authorization

Authorization is the process of controlling an individual's access to resources. Initial decisions regarding rights of an individual's access to Resources may be determined by administrative procedures or role-based privilege management. See IS-3, Electronic Information Security section III.C.1, Administrative Workforce Controls.

E. Level of Assurance (LoA)

The term "level of assurance" describes the degree of certainty that the individual who uses electronic credentials (identifier and authentication credential) is who that individual claims to be at the time of the authentication event. Assurance may be determined by factors such as:

- the degree of confidence in the vetting process used to confirm the identity of the individual to whom the credential was issued,
- the degree of confidence that the individual who uses the credential is the individual to whom it was issued,
- the degree of confidence of the security of the data exchange, and
- the degree of confidence that the authentication credential has not been shared with untrusted services.

Access to restricted information could require a higher level of assurance; Resource Providers may implement additional controls to increase Levels of Assurance. (See Section 7 in the NIST Special Publication 800-63, Electronic Authentication Guide.)

F. Enterprise Directory Services

An Enterprise Directory contains identity information about individuals who have been authorized to join a campus community. Enterprise directory services provide an essential infrastructure component that supports authentication and authorization to Resources.   Enterprise directories contain identity information, and they may also serve as repositories for electronic credentials or they may be integrated with systems that inform authentication or authorization events.

G. Single Signon Systems

Single Signon (SSO) describes a process that allows an individual to enter one set of electronic credentials for access to multiple Resources. A major goal of a SSO

system is increased efficiency and security through the reduction of multiple account management and less secure authentication processes.

Resource Providers should consider potential risks of SSO to protect against insecure user behavior, such as unauthorized sharing of authentication credentials. Additional authentication may be appropriate for access to specific resources that require a greater assurance of security.

Roles and Responsibilities for Identity and Access Management

IAM systems serve as a critical component of the campus security infrastructure. Campuses should work toward the development of systems and procedures to provide core automatic mechanisms that:

- insofar as possible, capture identity information from authoritative institutional repositories of information, such as from payroll or the student system,
- ensure timely provisioning and de-provisioning of access rights,
- offer self-service to facilitate individual's timely update of personal information and authentication credentials,
- ensure compliance through logging, auditing, and reporting.

A. Credential Provider

Each campus should designate an authorized Credential Provider to serve as the authoritative organizational unit that manages identity information and authentication services for a campus. When there is close affinity between locations, such as a campus and its medical center, it is recommended that they share a Credential Provider since implementing separate Credential Providers could cause confusion for individuals who belong to both communities.

Credential Providers are responsible for protection and authorized release of personal information consistent with law and University policy. See IS-2, Inventory, Classification, and Release of University Electronic Information and IS-3, Electronic Information Security for University guidelines.

Credential Providers should enable the following elements.

1. Identification

Verification that individuals are who they claim to be is fundamental to identity and access management. If possible, verification of identity should be conducted before identity information is entered into an authoritative institutional system. Insofar as possible, identification procedures should require that individuals present a government issued ID containing their picture and including an address or record of nationality, e.g., driver's license or passport. (Confirming identity of employees must conform to UC hiring policies and practices.)

- Individuals' identity information may be entered into institutional repositories through a variety of processes, such as during an application or hiring process. Note that the degree of confidence that the individual is who he or she claims to be influences the level of assurance of electronic credentials.

2. **Registration and Credentialing**

Since the process for vetting identity is closely related to registration and credentialing, procedures for coupling credentials to an identity should ensure accurate binding between the individual and the credentials.

- Registration procedures should ensure that the *authentication credential*, e.g., password, meets campus standards as required in IS-3, Electronic Information Security, section III.C.2.B Access Controls.

- Registration procedures should ensure that the electronic *authentication credential* is accurately bound to the individual's identifier and is issued by secure means only to the correct individual.

- Credential Providers should provide mechanisms that allow Resource Providers to implement timely provisioning and de- provisioning (termination) for Authorized Individuals' access to Resources.

- Where appropriate, Credential Providers should manage role and affiliate information for Resource Providers who grant access based on predefined roles, such as "student," "staff," "faculty," or "guest."

3. **Authentication**

The act of verification of the electronic credentials presented by the individual when accessing a Resource should be adequately protected.

- Appropriate encryption must be used to protect the privacy of the exchange when electronic credentials are transmitted during authentication.

- Measures should be established to prevent Resource Providers from having access to authentication credentials without prior authorization by the Credential Provider. Such authorization should ensure compliance with the Credential Provider's requirements for protection of the authentication credential.

4. **Enterprise Directory Management**

Although derived from distributed sources, the enterprise directory should be managed centrally. Procedures that ensure accurate life cycle management

of community members are a necessary component of enterprise directory management. Principles that enable the tracking of individuals through each phase of their affiliation with the campus, such as applicant to student, student to staff, or student to alumni, should be observed.

- Wherever possible, electronic information about individuals, including guests, in the enterprise directory should be maintained in a manner that ensures the proper verification of identities, facilitates automatic role assignment, and facilitates automated provisioning and de-provisioning of services.

- Procedures should be established that enable timely and accurate update of directory information, authentication credentials, and timely provisioning and de-provisioning of individuals or accounts.
    – The process of maintaining employee information should be integrated with University employment processes.
    – The process of maintaining student information should be integrated with student registration processing.

- Granting authorization must be consistent with University policy regarding Allowable Users as described in section III.C, Electronic Communications Policy.

5. **Documentation**

    Credential Provider's services should be fully documented, including requirements governing Resource Provider access to and use and protection of identity credentials. Documentation should include the level of assurance associated with authentication credentials and the practices used to achieve that level of assurance. Documentation should also include standards and best practices for use and protection of electronic credentials.

B. Resource Providers

Resource Providers are the organizational units that provide and manage electronic information services used to conduct University business by Authorized Individuals, such as financial or student information systems. These resources are generally network-based, but may not necessarily be so.

Resource Providers are responsible for appropriate protection of the information resources over which they have jurisdiction or control. For example:

- Resource Providers should establish procedures ensuring that only Authorized Individuals are permitted access to their Resources. For authorization management guidelines regarding workforce controls see section III.C.1, Administrative Workforce Controls in IS-3, Electronic Information Security.
- Resource Providers should ensure appropriate access control measures consistent with IS-3, section III.C.2, Operational and Technical Controls.

Resource Providers are responsible for appropriate protection of identity information they receive as part of the authorization and authentication processes.

If Resource Providers have access to or handle authentication credentials, their procedures and practices must be in full compliance with Credential Provider's requirements for handling and protection of those credentials.

Resource Providers should implement additional measures to enhance credential provider's level of assurance if Resource Providers require a higher level of assurance than that assigned by the Credential Provider.

C. Accountability

1. Administration

Administration of IAM systems requires that:
- Credential Providers implement procedures that ensure the documentation and appropriate retention of records linking individuals' names with their identification information in enterprise directories.
- Resource Providers implement appropriate audit logs that document individual access to Resources and the authorization permissions granted to individuals.

IAM systems should undergo periodic reviews to ensure confidentiality, integrity, and availability of the system.

2. Retention of Audit Logs

Log records provide essential detailed information that document many activities supporting information resources, such as the creation or editing of identity records, or recording of process transactions. Procedures for the retention of log records should be well-defined to provide an appropriate balance among the following:
- confidentiality of specific individual's activities,
- the need to support investigations,
- the cost of retaining the records.

When logs document or contain valuable information related to activities of the University's information resources or the people who manage those resources, they are University *Administrative Records*, subject to the requirements of the University Records Management Program. See RMP-2, Records Retention and Disposition and IS-3, Appendix C, Log Management.

Federated Identity and Access at UC

At the University of California, there may be need for community members from one campus to access services from another UC campus.   The University of California

utilizes [UCTrust](#), a federated approach to allow access to another campus by the use of authoritative identity information from the home location. It enables authorized campus individuals to use their local campus electronic credentials to gain access, as authorization permits, to participating services throughout the UC system.

Federated identity systems offer considerable benefits in efficiency and security for access to services offered at participating institutions.
- Convenience: individuals can access services of participating institutions using their local campus electronic credentials.
- Efficiency: federated systems reduce the overhead of maintaining multiple administrative tasks required for account maintenance since they utilize automated authentication and authorizations mechanisms.
- Privacy: federation reduces the need for creating multiple data stores of personal information. Participating campuses ensure the protection of personal information through secure access channels.

See UCTrust Service Description and Policies for participation requirements for both Credential and Resource providers.

IV.   COMPLIANCE / RESPONSIBILITIES

Systemwide
The Associate Vice-President – Information Technology Systems, 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.

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.

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.

Individuals and Community Members

Community Members are the individuals who have officially established an affiliation with a campus. They are the individuals who use the Resource Providers' services and whose electronic identity is managed by Credential Providers.

Community Members are responsible for protection of the electronic credentials provided to them by their Credential Provider. In particular, they are each individually responsible for:

- assurance that their credentials are not held by other people.
- compliance with Credential Provider's standards and best practices for use and protection of their electronic credentials.

Community Members are also responsible for conformance with Resource Providers' standards and best practices.

Community members 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.

V.   PROCEDURES

VI.   RELATED INFORMATION

- Electronic Communications Policy
- Management Guide for Information Security
- IS-2, Inventory, Classification, and Release of University Electronic Information
- IS-3, Electronic Information Security
- Policies Applying to Campus Activities, Organizations, and Students, Section 130.00.
- RMP-2, Records Retention and Disposition
- RMP-8, Legal Requirements on Privacy of and Access to Information

VII.   FREQUENTLY ASKED QUESTIONS

VIII.   REVISION HISTORY

This policy was last updated on July 27, 2007, and reformatted into the standard University of California policy template on May 11, 2012.