

University of California

Glossary of Terms in Selected Business and Finance Bulletins in the Information Systems (IS) Series

Administrative Operational Systems

Administrative operation systems are defined as those which use computers, including mainframe, servers, or desktop systems to collect, store, retrieve, and display information for use in the planning, management, and allocation of University information and resources.

Portable devices should only be used for administrative operational systems as necessary for collection or transmission of information. Restricted information may be retained on portable equipment only if protective measures, such as encryption, are implemented that safeguard the confidentiality or integrity of the data in the event of theft or loss of the portable equipment.

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.

Corporate Functions

Corporate functions are defined as those functions managed centrally for the benefit of the entire University, as opposed to those functions performed solely at local, campus sites. Examples of corporate functions are consolidated reporting, systemwide policy development, and compliance review.

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 Resource (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.

Encryption

The process of converting data into a cipher or code in order to prevent unauthorized access. The technique obfuscates data in such a manner that a specific algorithm and key are required to interpret the cipher. The keys are binary values that may be interpretable as the codes for text strings, or they may be arbitrary numbers. Appropriate management of these keys allows one to store or transmit encrypted data "in plain sight" with little possibility that it can be read by an unauthorized entity. For example, encryption can protect the privacy of restricted data that is stored on a laptop computer, even if that laptop computer is stolen. Similarly, it can protect data that is transmitted, for example, over a network, even if that network is tapped by an unauthorized third party

Essential Resource

A Resource is designated as Essential if its failure to function correctly and on schedule could result in (1) a major failure by a Campus to perform mission-critical functions, (2) a significant loss of funds or information, or (3) a significant liability or other legal exposure to a Campus.

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.

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

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.

Restricted Resource

A Resource that supports the storage, transmission, or processing of restricted information to which access requires the highest degree of restriction and that requires the highest level of security protection. 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.

Stewardship of Electronic Information Resources

Stewardship is an ethic that embodies the act of conscientious management, protection, and care of valuable University electronic information resources.