UNIVERSITY
OF
CALIFORNIA

UCOP
ITS
Systemwide CISO Office
Systemwide IT Policy

IT Policy Glossary

Revision History

Date:	By:	Contact Information:	Description:
06/28/2007	Stephen Lau		The UC-IT-00-0410_glossary PDF was archived on 1/17/2019. The obsolete terms were going to be merged into the 2018 Glossary and then purged when the polices that reference them were replaced.
2018	Robert Smith	robert.smith@ucop.edu	Edited to make IS-3 and Glossary match on key terms. Consolidated terms from the 2007 version of the glossary into this version. Completed addressing comments from Academic Senate 1/17/18 meeting. Adjusted definitions to have a consistent style. Made small updates to ensure consistency with Disposal Standard.
Sept 2019	Robert Smith	robert.smith@ucop.edu	Added deprecated terms from 2007. Minor formatting changes. Addressed UC Berkeley comments on IT Resources. Added three definitions. Updated definition of IT Resources.
August 2021	Robert Smith	robert.smith@ucop.edu	Added terms from IS-12. Added examples for definitions for IS-12.

05/11/2023	Robert Smith	robert.smith@ucop.edu	Added revision history and index. Updated the formatting.

The IT Policy Glossary includes defined terms relevant to using UC’s IT and information security policies and standards.

It defines terms related to a variety of topics, including but not limited to, the roles of Workforce Members; the processes by which information is kept secure; and the classification of data, resources and information to be protected. If a term isn’t found in the IT Policy Glossary, then use industry normative definitions and understandings.

Table of Contents

Systemwide IT Policy Glossary

Term	Definition
Acceptable Use	A term referring to usage of Institutional Information and IT Resources that complies with UC's security, privacy, and ethics policies. Acceptable use is defined based on a variety of factors. For example, a Workforce Member's (employee's) acceptable use policy may differ from a student's or guest's acceptable use policy. Example 1: The library offers complimentary wireless access to visitors. As part of the registration process, users review and agree to abide by the terms that govern the use of this access, including the rule not to access or attempt to access UC IT Resources or facilities without proper authorization, and not to intentionally enable others to do so. Example 2: Housing and Events offers complimentary wireless access to event attendees. As part of the registration process, users review and agree to abide by the terms that govern use of this access, including the rule not to run programs that attempt to calculate or guess passwords, or that are designed to trick users into disclosing their passwords.
Administrative Operational Systems (Deprecated)	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. Last used: 2007.

Systemwide IT Policy Glossary

Term	Definition
Affiliate	An individual who requires access to IT Resources or Institutional Information but is not explicitly paid by UC. Affiliates comprise a wide range of individuals, including contractors, visiting scholars, and retired Workforce Members who wish to retain service access. Affiliate status for individuals other than UC students, faculty or staff requires authorization by the appropriate Unit. The status might include individuals in program, research, contract, or license relationships with UC. Example 1: A visiting Ph.D. scholar who is in residence at a Location to conduct independent research and is not receiving payment from UC can be considered an Affiliate. Example 2: A Supplier, on site to conduct repairs, requires network access to run diagnostics and perform online troubleshooting. This Supplier can be considered an Affiliate.
Authorized Individual (Deprecated)	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. Last used: 2007.
Availability Level	1. The degree to which Institutional Information and IT Resources must be accessible and usable to meet business needs. 2. Timely and reliable access to and use of accurate information.

Term	Definition
	Example 1: Active Directory (AD) is used for sign-on to 20 separate applications and requires a high level of availability. Example 2: The Electronic Medical Record (EMR) system is used by medical center operations and requires a high level of availability. Example 3: Streaming music for a dining patio requires a low level of availability. Example 4: A website containing press releases from the previous five years requires a low level of availability. Example 5: A website containing upcoming event details requires a moderate level of availability. See the Availability Level Classification Guide for additional examples.
Breach	1. Any confirmed disclosure of Institutional Information to an unauthorized party. 2. Unauthorized acquisition of information that compromises the security, confidentiality, or integrity of Institutional Information maintained by UC. 3. The electronic acquisition, access, use, or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule. Example 1: A breach has occurred if credit card numbers are harvested from a point of sale system.

Term	Definition
	Example 2: A breach has occurred if usernames and passwords are harvested from a campus server. Example 3: A breach has occurred if a USB drive containing prospective and current students' names and personal information is stolen. Example 4: A breach has occurred if a ransomware attack results in the loss of availability of electronic protected health information (PHI).
Business Continuity Plan (BCP)	Documented procedures that guide organizations on how to respond, recover, resume, and restore business to a pre-defined level of operation following disruption. BCP is also known as a "continuity plan" in the UC Ready tool and, in other tools, Continuity of Operations (COOP). Example 1: A Location creates a written document that identifies critical operations and risks, provides a set of steps to maintain or restore critical operations during a crisis, and documents how to communicate with key people during the crisis. Example 2: The written preparation specifying the steps to continue to provide our essential services with as little disruption as possible during unexpected events on the campus, such as floods, fires, and damaged server rooms. Example 3: The Financial Aid department has a written plan to process financial aid using a redundant site in another state. Example 4: A UC Central IT Unit has a written plan to recover both locally and at the fail-over site, the San Diego Supercomputer Center (SDSC) keeping the enterprise functional no matter where it is being executed,

Systemwide IT Policy Glossary

Term	Definition
	locally or remotely, and ensures that the enterprise functionality will be available to its customers and users.
CIO	A Chief Information Officer (CIO) is a senior executive responsible for information technology or information system functions throughout a Location. Example: An IT Leadership Council member from a campus can be the CIO.
CISO	A Chief Information Security Officer (CISO) is a role responsible for security functions throughout a Location, including assisting in the interpretation and application of this policy. For some Locations, the title may be Information Security Officer (ISO). ISO and CISO are equivalent terms for policy application purposes. Example 1: A UC campus appoints an Information Security Officer and assigns responsibilities outlined in this policy. Example 2: A UC campus appoints two CISOs: one for its main campus and one for the hospital and medical school. Each CISO is assigned the responsibilities outlined in this policy. Example 3: A UC Location appoints two people to act in the role of CISO dividing responsibilities to meet the needs of the Location.
Clear	A disposal process using software or hardware products to overwrite storage space on media. Clear may include overwriting not only the logical storage location of a file(s) (e.g., file allocation table), but also all addressable locations. Clear also protects against keyboard based or simple non-invasive data recovery techniques.

Term	Definition
	Example 1: A software application Clears when it writes a stream of zeros, ones, or pseudorandom data onto all sectors of a hard disk drive. Example 2: A data eradication program Clears when it performs multiple overwrites using random or proven data patterns supporting recognized government and industry standards. Example 3: Darik's Boot and Nuke, also known as DBAN, is an open-source project hosted on SourceForge. The program is designed to securely erase a hard disk so the original data is permanently removed and no longer recoverable. This is known as Clearing. Example 4: SDelete (Secure Delete) can securely delete existing files, as well as securely erase any file data that exists in the unallocated portions of a disk. This is known as Clearing.
Confidential Information (Deprecated)	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. Last used: 2007.

Term	Definition
Corporate Functions (Deprecated)	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. Last used: 2007.
CRE	Cyber-risk Responsible Executive (CRE) is an individual in a senior management or academic position who reports to the Location chancellor or top Location executive. The CRE is accountable for all information risk assessments, security strategies, planning and budgeting, incident management, and information security implementation. Example 1: A Provost can be assigned the role of CRE. Example 2: Chief Financial Officer (CFO) can be assigned the role of CRE. Example 3: Chief Information Officer (CIO) can be assigned the role of CRE. Example 4: A senior faculty member serving on the Chancellor’s staff can be assigned the role of CRE.
Credential Providers (Deprecated)	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. Last used: 2007.

Systemwide IT Policy Glossary

Term	Definition
Critical IT Infrastructure	1. IT Resources that manage unrelated sets of Institutional Information or sets of large or particularly sensitive Institutional Information. 2. IT Resources that meet two conditions: a) Several information systems rely on the resource such that a security issue with the resource would affect multiple systems. b) The default or standard method for securing the system is inappropriate due to an elevated level of risk, complexity, or the specialized nature of the IT Resource. Example 1: Active Directory, which maintains information about users, permissions, and other security-related attributes, is considered Critical IT Infrastructure. Example 2: A single departmental server performing many critical functions. The combination of these functions results in a system that requires special security measures is considered Critical IT Infrastructure. Example 3: An encryption key management system protecting keys for many systems is considered Critical IT Infrastructure. Example 4: A firewall protecting Electronic Medical Record (EMR) system databases is considered Critical IT Infrastructure. Example 5: A Domain Name System (DNS) outside of central IT is considered Critical IT Infrastructure. Example 6: Wired and wireless networking equipment that provides access to Institutional Information protected by regulation or contract, such as health information or credit card track data, is considered Critical IT Infrastructure.

Term	Definition
Cryptographic Erase (CE)	A disposal process that safely destroys all copies of the decryption key. If all data is adequately encrypted, then once the decryption key is removed, the Institutional Information is not recoverable. Example 1: The target data is encrypted. Once the decryption key is securely deleted (Sanitized), the data is inaccessible. This is a Cryptographic Erase. Example 2: iOS devices use Cryptographic Erase when the "Erase all content and settings" option is used. This option discards all the keys in effaceable storage, thereby rendering all user data on the device cryptographically inaccessible.
Cyber Incident Escalation Protocol	A required process used to ensure that appropriate incident communication occurs at the Location and from the Location to the UCOP cyber leadership team, UCOP supporting departments/functions and the Regents of the University of California.
Degauss	A disposal process that 1) erases data by using a formalized technique that alters the magnetic storage of information in such a way that it cannot be accessed or recovered or 2) reduces the magnetic flux to virtual zero by applying a reverse magnetizing field. To reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Example 1: A machine that alters magnetic data storage devices by changing the magnetic domain is a degausser. Data on the degaussed device is unreadable.

Term	Definition
	Example 2: A process that exposes magnetic media to a magnetic field that erases or demagnetizes the media, leaving it magnetically blank or scrambled, is degaussing. Data on these devices is unreadable.
Delete	A disposal process that removes the ability to access the respective file, record, or data in the operating system or application. Example 1: On a Windows or MacOS device, a user deletes a file by moving it to the trash/recycle bin and then empties the trash. Example 2: In a relational database, using SQL TRUNCATE TABLE is a Delete. Example 3: In a relational database, using the SQL DROP TABLE is a Delete.
Destroy	A disposal process that makes media not usable again and renders Institutional Information irretrievable even using specialized recovery techniques. It also results in the subsequent inability to use the media for storage of data (e.g., shred, disintegrate, pulverize, or incinerate by burning the device in a licensed incinerator). Example 1: An industrial shredder that physically cuts media or devices into small parts that cannot be reassembled. This is an example of Destroy. Example 2: An industrial incinerator uses intense heat to consume media or devices, reducing them to ash or particulate. This is an example of Destroy.
Electronic Information Resource (Deprecated)	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

Term	Definition
	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. This term has been replaced by IT Resource (see below). Last used: 2007.
Emergency Change	A change that must be deployed as soon as possible due to a critical need, such as protecting the Location from a threat or fixing an IT service error that is causing a major impact to business. Documentation and reviews are produced after the change. Example 1: A vendor requires the application of a patch to resolve a major outage. This constitutes an emergency change. Example 2: A critical application is down and the technical team requires the installation of a diagnostic tool to troubleshoot the problem, which is considered an emergency change.
Essential Resource (Deprecated)	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. Last used: 2007.
Essential System	A system required for the operation of a major function at a Location. See IS-12 for a detailed explanation.
Event	See Information Security Event.

Systemwide IT Policy Glossary

Term	Definition
Evidence-Based Approach	The conscientious, explicit, and judicious use of evidence to demonstrate compliance or performance. Example: The system Risk Assessment requires monthly vulnerability testing. The requirement is calendared, and each month a ticket is opened and assigned. A scan is run and the output is attached to the ticket. Each remediation ticket references the scan ticket. The calendar entry, the ticket for the scan, the scan results, and the ticket(s) for remediation all show evidence of compliance.
Guideline	A collection of system-specific or procedure-specific recommendations for best practices. Guidelines are strongly recommended practices or steps, but are not required. Example 1: The Microsoft Windows hardening guide is a guideline. Example 2: A vendor's best practice guide for securing a system is a guideline.
Hash (Hash Function)	A value computed from a cryptographic function that maps a string of characters of arbitrary length (passphrase + salt) to a fixed-length bit string (the hash value). Example 1: A function that can be used to map data of an arbitrary size to data of a fixed size, such as SHA-1 or SHA-256, is a Hash. Example 2: A function that can be used to map data of variable size to data of a fixed size, such as MD-5, is a hash.
Implementer	The Workforce Member responsible for developing, implementing or configuring a system or IT Resource.

Term	Definition
	An Implementer can come from a Unit, Service Provider or Supplier. The Unit Information Security Lead may play this role when acquiring a system or service. Example 1: A Workforce Member who sets up a cloud based application for use by one or more Units is an Implementer. Example 2: A Workforce Member who installs an IT Resource is an Implementer.
Incident	See Information Security Incident below.
Information Security Event (Security Event)	1. An identified occurrence in a system, service, or network state indicating a possible breach of information security policy, a failure of controls, or a previously unknown situation that may be relevant to security. 2. An alert or notification created by a person, IT service, configuration item or monitoring tool related to information security. These typically require IT operations personnel to investigate or act and can lead to an Information Security Incident (see definition below). Example 1: Antivirus software sends an alert when malware is detected. This is a security event. Example 2: Firewall logs show remote connection attempts from an unexpected location. These are security events. Example 3: Windows recording the creation of a new local administrator account on a point-of-sale terminal is a security event.

Term	Definition
	Example 4: A supervisor reports that a user found a way to redo a transaction that should be otherwise locked. This is a security event.
Information Security Incident (Security Incident)	A compromise of the confidentiality, integrity, or availability of Institutional Information in a material or reportable way. A single event or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations or threatening information security. Example 1: A stolen laptop that contains unencrypted, personally identifiable information is a Security Incident. Example 2: An attacker prevents the medical record system from functioning for patients and practitioners. This is a Security Incident. Example 3: An attacker takes personnel data from a payroll system, which is a Security Incident. (Note: This is also an example of a Breach). Example 4: A UC Workforce Member takes records of individuals simply for curiosity and to learn what they are doing. This is a Security Incident.
Information Security Incident Response Plan	An Information Security Incident Response Plan is the written document detailing the steps required to address and manage an Incident or cyber attack. Example 1: The Location document describing how it will respond to an Incident is an Information Security Incident Response Plan. Example 2: The Unit document describing how it will respond to an Incident is an Information Security Incident Response Plan.

Term	Definition
Information Security Incident Response Program	The full, comprehensive effort to identify, prevent, prepare for, respond, and recover from Incidents or cyber attacks. Example 1: The Location’s incident response plan combined with the overall strategy to identify and govern assets, protect IT Resources, detect adverse events, respond to attacks, recover from damage, and allocate resources is known as the Information Security Incident Response Program. Example 2: The Unit’s organized approach to prepare for, detect, address, and manage the aftermath of a security breach or cyber attack is called its Information Security Incident Response Program.
Initiator	A Workforce Member who identifies the need to classify the Protection Level and/or Availability Level of Institutional Information or IT Resources. A wide range of Workforce Members can become Initiators when they acquire an application or system, or when they create or collect Institutional Information. Example 1: The Student Affairs IT group requests an extract from the student information management system to populate another system. Student Affairs IT is the Initiator. Example 2: A financial analyst creates a new reporting dashboard on investment performance using analysis and modeling she developed. The financial analyst is the Initiator. Example 3: A project manager is working with a third-party Supplier to develop a wellness application. The application requires an aggregation of data from the student recreation center and the student information management system. The project manager is the Initiator.

Systemwide IT Policy Glossary

Term	Definition
Institutional Information	A term that broadly describes all data and information created, received and/or collected by UC. Example 1: Information contained in a database, such as employee personnel records or records pertaining to student enrollment and grades, is Institutional Information. Example 2: Activity log data from a server application or network device is Institutional Information. Example 3: Emails sent and received pertaining to UC business are considered Institutional Information. Example 4: Instrument measurements from academic research, collected manually or electronically, are Institutional Information. Example 5: Electrical use data collected by a building automation system is Institutional Information.
Institutional Information Proprietor	See Proprietor.
Integrity	The consistency, accuracy, and trustworthiness of data over its entire lifecycle. Example 1: An application administrator changes records to cover mistakes, causing a loss of integrity. Example 2: A technician makes changes to a report she wasn’t authorized to access, causing a loss of integrity.

Term	Definition
	Example 3: A storage device crashes and leaves files corrupted, causing a loss of integrity. Example 4: Data transmitted over a network or written to storage can have errors and become corrupt. Checksums (mathematical features in protocols and devices) are used to detect and often correct errors, which maintains the integrity of the data. Example 5: File permissions are set to allow only those authorized to change data in a file. This type of control protects the integrity of the data by allowing only authorized users to make changes.
ISMP	Information Security Management Program (ISMP) is an overall program of identifying and managing information security risk within established UC and Location tolerances. The ISMP identifies the requirements for a Location-wide information security program and describes the established or planned management controls and common controls for meeting those requirements. It combines elements related to cyber security to manage risk to acceptable levels. This includes management commitment, policies, standards, procedures, work instructions, tools, systems of record, guidelines, and checklists. Example 1: A Location creates and documents an overall program that maps system-level requirements to local procedures, provides governance and risk management information, maps key roles to IS-3 roles, lists key contacts, and identifies resources for compliance. This is an ISMP. Example 2: Student Affairs IT creates and documents a program explaining policies, work instructions, risk management, tools, conventions, training,

Term	Definition
	personnel requirements, and contractual requirements. This is an ISMP for Student Affairs. Example 3: This ISMP is a systematic approach to managing sensitive Institutional Information so that it remains secure. The ISMP includes people, processes, and IT systems by applying a risk management process.
ISO (Information Security Officer)	See CISO.
ISO 27000/International Organization for Standardization 27000	ISO is an independent, non-governmental international organization with a membership of more than 150 national standards bodies. Through its members, ISO brings together experts to share knowledge and develop voluntary, consensus-based, market relevant International Standards that support innovation and provide solutions to global challenges. ISO 27000 includes a collection of information security standards intended to help an organization implement, maintain, and improve its information security management. Example 1: ISO 27002:2013 is a comprehensive set of controls focused on information security. Example 2: ISO 27005:2013 is focused on information security risk management.
IT Recovery	A term that includes all activities needed to enable access to Institutional Information and enable business functions. This includes: • IT Disaster Recovery – recovering the operating state of IT Resources and access to Institutional Information

Term	Definition
	(information systems or cloud services) that support identified business functions. - IT Service Continuity – restoring or making available equivalent functional IT Resources and access to Institutional Information, whether temporary or durable, that support identified business functions. Example 1: Planning, procedures, and tools that enable the restoration of IT services to support mission delivery. Example 2: Restoring IT or technology systems supporting critical business functions, as opposed to business continuity, which involves keeping essential aspects of a business functioning despite significant disruptive events. IT Recovery can therefore be considered a subset of business continuity. Example 3: An organization's method of regaining access and functionality to its IT infrastructure after events like a natural disaster, cyber attack, or even business disruptions related to a pandemic. Example 4: A recorded set of steps and/or processes that are designed to assist an organization in executing recovery in response to a disaster to protect mission delivery, including Institutional Information and IT Resources.
IT Resource(s)	A term that broadly describes IT infrastructure, software and/or hardware with computing and networking capability. These include, but are not limited to: portable computing devices and systems, mobile phones, printers, network devices, industrial control systems (SCADA, etc.), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic media, Logical Media,

Term	Definition
	biometric and access tokens and other devices that connect to any UC network. This includes both UC-owned and personally owned devices while they store Institutional Information, are connected to UC systems, are connected to UC Networks, or are used for UC business. Example 1: A Cisco firewall installed in a data center or building communications room is an IT Resource. Example 2: An electrical and temperature monitoring system used for a building's LEEDS certification is an IT Resource. Example 3: A video camera surveillance system is an IT Resource. Example 4: A database server is an IT Resource. Example 5: A network-attached printer, scanner, and copier are IT Resources. Example 6: A computer, including a laptop, server, or point-of-sale system is an IT Resource. Example 7: A personal smartphone used to access UC email or store Institutional Information is an IT Resource. Example 8: A personally owned PC used to conduct UC business remotely is an IT Resource.

Term	Definition
	Example 9: Personally owned computers, tablets, or other devices connected to non-public campus networks or used to process, store, or transmit Institutional Information are IT Resources. Example 10: IaaS (Infrastructure-as-a-Service), PaaS (Platform-as-a-Service, SaaS (Software-as-a-Service), or other “as-a-service” instance(s) (e.g., Storage, Database, Information, Process, Application, Integration, Security, Systems Management, or Testing) are IT Resources. Example 11: The composite hardware, software, network resources, cloud resources (public, private, or hybrid), and associated electronic information services used to process, store, transmit, create, or manage Institutional Information are IT Resources. Example 12: Enterprise or Unit applications like webservers, FTP servers, mail servers, file servers, directory servers, logging servers, messaging servers, communication servers, video servers, and other electronic services used to process, store, transmit, create, or manage Institutional Information are IT Resources.
IT Workforce Member	A Workforce Member who is assigned specific information technology (IT) duties or responsibilities. Example 1: The student recreation center employs a dedicated office manager who also has IT duties. Since the role includes IT responsibilities, this person is considered an IT Workforce Member. Example 2: A UC business school employs a multimedia technician. Role responsibilities also include PC and equipment installation, patching, software installation, and event support. Since the role includes IT duties, the technician is an IT Workforce Member.

Term	Definition
	Example 3: The housing lock shop manages a wide range of electronic locks, servers, consoles, and video systems. The lead technician supports these systems and manages the vendor contracts. Since the role includes IT duties, the technician is an IT Workforce Member. Example 4: The central IT group has a group of database administrators. Since the role includes IT duties, the administrators are IT Workforce Members.
Least Privilege Access	The practice of limiting access to the minimum level that will allow normal functioning. Applied to Workforce Members, this principle translates to giving people the minimum level of access rights they require to do their jobs. Applied to security architecture, each entity is granted the minimum system resources and authorizations it needs to perform its function. Example 1: A cashier in a residential dining hall only needs permission and rights to log in to the register. Following the principle of Least Privilege Access, the cashier does not have access to the register's operating system or its administrative functions because he does not need it to perform his duties. Example 2: A financial analyst runs a monthly vacation and leave report for department managers. Someone else developed the report. Following the principle of Least Privilege Access, the department created a special role in the reporting system that allows the analyst to run the vacation and leave report without accessing any other data.

Term	Definition
	Example 3: A program monitors a directory on a local machine for a file. Following the principle of Least Privilege Access, the directory permissions are set so that the program can run using a restricted account with only access to that directory. Example 4: The front desk attendant in the Financial Aid Department has access to the sign-in system, which provides basic information about the appointment holder, the waiting area to use, and the likely wait time. According to Least Privilege Access, the attendant can read, but not update, the records because updating is not required for their work.
Location	A discrete organization or entity governed by the Regents of the University of California. Locations include, but are not limited to: campuses, laboratories, medical centers and health systems, as well as satellite offices, affiliates, or other offices controlled by the Regents of the University of California. Example 1: A specific UC campus is a Location. Example 2: A geographically separated office is a Location, such as the UC Path office in Riverside, California. Example 3: The University of California's Office of Federal Governmental Relations located at the UC Washington Center in Washington, D.C. is a Location. Example 4: The San Diego Supercomputer Center, an Organized Research Unit of the University of California, San Diego is a Location.

Term	Definition
Logical Delete	A disposal process of non-destructive deletions of data, records, or information within applications. The information is marked as "deleted" and may not be exposed to users, but some data may still be recoverable. Example 1: Emptying the trash or recycle bin in operating systems is a Logical Delete. Example 2: In LINUX and similar operating systems, the 'rm' command is a Logical Delete. Example 3: A delete marker in versioned storage, such as Amazon S3, is a Logical Delete. Example 4: A soft delete that keeps the data for a certain number of days, as done in Google Cloud Storage, is a Logical Delete.
Logical Media	A set of data independent of the physical media on which it is recorded. Example 1: A disk partition in Windows is Logical Media. Example 2: A volume in LINUX is Logical Media. Example 3: A Storage Adapter in VMWare is Logical Media. Example 4: An S3 Bucket in Amazon is Logical Media. Example 5: Google Drive is Logical Media.
Maximum Tolerable Downtime (MTD)	The amount of time a mission/business process can be disrupted without causing significant harm to the Unit or Location's mission.

Term	Definition
	Example 1: The Student Health Services Director determines that the longest time the clinic can operate without the medical records system is one business day. Example 2: With input from key stakeholders, the Provost determines the learning management system used to support instruction can be down for no more than two calendar days without impacting the learning mission. Example 3: The CIO, after consulting key stakeholders, determines that core network services should be designed and delivered with full redundancy and resilience to prevent outages greater than 5 minutes.
Multifactor Authentication (MFA)	An authentication system that requires more than one distinct authentication factor for successful authentication. Multifactor authentication can be performed using a multifactor authenticator or by a combination of authenticators that provide different factors. Example 1: An application used to authorize access on a second device that the Workforce Member possesses is a type of Multifactor Authentication. Example 2: A device specifically designed to provide a random number or code used to log in, also known as a token, is known as a type of Multifactor Authentication. Example 3: A two-step verification using a code texted or called to the user is a Multifactor Authentication process.
Need-to-Know	1. A method of isolating information resources that a user requires to do their job, but no more.

Term	Definition
	2. A security, privacy, HIPAA, and FERPA principle that requires access to data be granted based on a legitimate business justification, typically to perform a specific job duty. HIPAA refers to this as the “Minimum Necessary Requirement.” The HIPAA Privacy Rule generally requires UC to take reasonable steps to limit the use or disclosure of and requests for protected health information to the minimum level necessary to accomplish the intended purpose. According to FERPA, a legitimate educational interest is necessary for a Workforce Member to carry out their responsibilities in support of UC's educational mission. Legitimate educational interest is a "need-to-know" that is essential to carrying out job responsibilities related to education. Example 1: After going through the correct process, Sam, a UC student and information security intern, is authorized by the CISO to perform an investigation into the compromise of a system in University Advancement. Sam can collect and evaluate the websites visited because he has a legitimate and approved reason to do so, i.e. he has a “need-to-know.” Example 2: The Registrar has determined that all Registrar’s office staff need access to student schedules and grades to do their jobs, i.e., they have a “need-to-know.”
Normal Change	1. A change that follows the defined steps of the change management process and includes required documentation and reviews. 2. A change that is not an emergency change or a standard change. Example 1: A software development team completes a new sign-in application for offices on campus. The application is expected to be

Term	Definition
	available for users in two weeks. The project manager completes all paperwork for approval. This is a normal change. Example 2: A Location’s Facilities Department has scheduled a vendor to replace 25 video cameras in parking garages and near parking pay stations and all required project documentation is complete. Paperwork, supporting documentation, and reviews are complete. This is a normal change. Example 3: A new application is ready for deployment. All required documentation is complete and all reviews are complete. The system owner requests that the application be deployed as a normal change. Example 4: A new wireless access point (WAP) is ready to be deployed. All required documentation and reviews are complete. The Network Manager requests approval for installing the new WAP as a normal change.
Passphrase	A sequence of words or other text used as part of the authentication process. A passphrase is similar to a password in usage but is generally longer for added security. Example 1: “127 SHARKS are more dangerous than 12 guppies?” is a passphrase. Example 2: “My son Sam, is funny when he spits carrots!” is a passphrase.
Password	1) A string of characters (letters, numbers and/or symbols) used to authenticate an identity, verify access authorization, or derive cryptographic keys. Generally composed of not more than 8-16 characters. 2) A type of memorized secret.

Term	Definition
	3) A type of authenticator comprised of a string of characters intended to be memorized or memorable by the user, permitting the user to demonstrate something they know as part of an authentication process. Example 1: $gr33nEGGSnH is a password. Example 2: 21beatsAC3@ is a password.
Personal Identification Number (PIN)	A memorized secret typically consisting of numerical digits. Example: 687591 is a PIN.
Physical Media	The tangible, physical materials or devices that are used to store or transmit Institutional Information. They can be touched and felt, having physical properties, such as weight and color. Example 1: Hard drives are physical media. Example 2: Rewritable optical media (e.g., CDs and DVDs) is physical media. Example 3: USB drives are physical media. Example 4: Tapes and tape cartridges are physical media. Example 5: Solid state drives are physical media.

Term	Definition
Procedure	1. A collection of steps or processes that describe how the requirements of a specific job task, policy, or standard are met. 2. Documentation of required steps and activities necessary to adequately and consistently carry out critical information security processes. Example 1: The detailed steps and reviews required to approve a change request constitute a procedure. Example 2: The detailed steps required to grant a new employee access to the network and systems constitute a procedure.
Proprietor	1. The individual responsible for the Institutional Information and processes supporting a University function. Proprietor responsibilities include but are not limited to: ensuring compliance with University policy regarding the classification, protection, access to, and release of information according to procedures established by UC, the Location, or the department, as applicable to the situation. 2. The individual responsible for the IT Resources and processes supporting a University function. Proprietor responsibilities include but are not limited to: ensuring compliance with University policy regarding the classification, protection, access to, location, and disposition of IT Resources. 3. An identified group, committee, or board responsible for the Institutional Information and processes supporting a University function. Proprietor responsibilities include but are not limited to: ensuring compliance with University policy regarding the classification, protection, access to, and release of information according to procedures established by UC, the Location, or the department, as applicable to the situation.

Term	Definition
	Example 1: The Registrar is the Proprietor of student data. Data extracted from a student information system (SIS) and loaded into the student recreation center (SRC) management system is still governed by the Registrar. The SRC cannot then release the data to a wellness program without review and approval by the Proprietor (Registrar). Example 2: The Math Department has acquired appropriate approval from the Registrar to obtain an SIS extract of students who are taking a series of science, technology, engineering, and math classes. The Chemical and Environmental Engineering Department later asks the Math Department for the data for a similar analysis. Since the department is not the Proprietor, the Registrar must approve the transfer. Example 3: A social sciences professor asks for a data dump from the system supporting Greek organizations. The dean of students, or designee, is the Institutional Information Proprietor and must review the request to determine the rules for approval or denial. Example 4: University Advancement acquired student data from various colleges on campus, including majors, degree dates, and GPA scores. It also purchased alumni data from third parties to aid fundraising efforts. Advancement is considering a cloud-hosted third-party system. The executive director wants to determine what protections are required for the data. The Proprietor for the purchased data is the executive director of University Advancement, and the Proprietor for student data related to graduation, majors, and GPA is the Registrar. Therefore, the executive director of University Advancement needs to work with the Registrar to classify the data. Example 5: The press called the campus Public Affairs Department to get detailed admissions data for the upcoming year. The Public Affairs

Term	Definition
	Department contacts the director of admissions, who is the Proprietor for this information. Public Affairs will work with the director of admissions to determine what information can be released to the media. Example 6: The Principal Investigator of an identifiable human subject research project is a Proprietor.
Protection Level	An assigned number representing the level of protection needed for Institutional Information or an IT Resource. The scale goes from the minimum level of protection (Protection Level 1) to the highest level of protection (Protection Level 4) and is based on the potential harm resulting from unauthorized access, disclosure, loss of privacy, compromised integrity, or violation of external obligations. Example 1: Public website data is intended for public availability and only needs the minimum protection level required for all Institutional Information and IT Resources. No concerns exist regarding who views the information classified as Protection Level 1. Integrity concerns do exist, however, so appropriate protection must be in place. Example 2: Electronic Medical Records are subject to specific regulatory and statutory requirements to protect patient privacy. These records require the highest level of protection (Protection Level 4). Example 3: A researcher is collecting human subject data. The data set initially contains personally identifiable information covered by HIPAA or state regulations. The researcher plans to later de-identify the data. Until the data is fully de-identified, it will require the highest level of protection (Protection Level 4) due to statutory requirements for protecting specific types of personal information.

Term	Definition
	Example 4: A researcher receives a federal grant. The grant requires compliance with several data protection guidelines and standards that generally correspond to UC Protection Level 3. The project will be classified according to these external obligations. See the Protection Level Classification Guide for additional examples.
Public Information (Deprecated)	Public information is any information relating to the conduct of the public's business. 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. Last used: 2007.
Purge	A disposal process that makes the media reusable but makes accessing the Institutional Information infeasible. This applies to physical or logical techniques that render Institutional Information recovery unachievable. Purge protects against laboratory attacks. Executing the secure erase firmware command on a disk drive, Cryptographic Erase and Degaussing are acceptable methods of purging. Example 1: Executing the secure erase firmware command on a disk drive is a type of Purge. Example 2: Degaussing is a type of Purge.
Recovery Point Objective (RPO)	The amount of data that can be lost before significant harm to the business occurs. The objective is expressed as a time measurement from the loss event to the most recent backup preceding the event. Example 1: The Registrar determines that, while not desirable, the course registration process could accept the loss of two days' data, which would

Term	Definition
	require students who registered for classes or who changed their schedule to have to do so again. The RPO is 48 hours – the backup interval is 48 hours or less. Example 2: The Transportation and Parking Services director determines that the system storing and processing parking ticket data could afford to lose one weeks' data. The RPO is 7 days – the backup interval is 7 days or less.
Recovery Time Objective (RTO)	The length of time allowed for the restoration of business processes and the achievement of a stated level of service following a disruption.
Researcher	A UC faculty member conducting research on behalf of UC. A researcher is also a Workforce Member. Example 1: Principal investigator or other designation paid by UC is a Researcher. Example 2: Collaborators at other institutions who are creating, securing, and maintaining UC Institutional Information are Researchers. Example 3: Staff research assistants are Researchers. Example 4: A graduate student who is performing research and is creating, securing, and maintaining UC Institutional Information is a Researcher.
Resource Custodian (Deprecated)	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

Term	Definition
	departmental databases. This role provides a service to the Resource Proprietor. Last used: 2007.
Resource Proprietor (Deprecated)	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. Last used: 2007.
Resource Providers (Deprecated)	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. This term has been replaced by Service Provider (see below). Last used: 2007.

Systemwide IT Policy Glossary

Term	Definition
Restricted Information (Deprecated)	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. Last used: 2007.
Restricted Resource (Deprecated)	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. Last used: 2007.
Risk Assessment	A process to identify, rate, and prioritize risk, as well as to document risk tolerance. Example 1: A Unit identifies the likelihood and impact of possible specific harmful cyber events and uses these ratings to define risk levels for each event. The ratings identify and prioritize risks requiring action. The department develops a spreadsheet to facilitate and document the process and outcomes, as well as to increase the visibility of risks and assist management in making decisions. Tabs in the spreadsheet guide the process and ask relevant questions. These steps and procedures form a Risk Assessment. Example 2: A Location adopts an IT governance, risk management, and compliance (GRC) tool. The GRC tool has workflows and risk rating systems

Term	Definition
	to help identify, prioritize, and manage information security risks. Units complete assigned tasks in the tool. These steps and procedures form a Risk Assessment.
Risk Treatment Plan	1. A pre-approved plan to provide a standard, scalable, and repeatable response to address pre-identified risks in a specific situation. 2. A set of information security controls and practices that manage risk within established UC and Location tolerances. Example 1: The Dining Department, a Unit, is adopting a network-connected time clock that interfaces with the campus time and attendance reporting system. While this system does not provide payroll functions, it does interface with the payroll system. The Unit develops a Risk Treatment Plan for the time clocks that identifies the required technical and administrative controls. The CISO approves the Risk Treatment Plan. The Dining Department and other Units can now install additional time clocks following the pre-approved Risk Treatment Plan. Example 2: A central IT department sets a new standard for network switches. IT, units, and contractors will install hundreds of these switches across the campus in the coming months. The IT team works with the CISO to develop a Risk Treatment Plan for the switch that identifies the required technical and administrative controls. Each unit and contractor can rely on the standard Risk Treatment Plan for each installation.
Risk-Based Approach	1. A process of allocating resources and defenses proportionate to the risks present in a specific context. 2. A process for managing information security risk including: (i) a general overview of the risk management process; (ii) how organizations establish the context for risk-based decisions; (iii) how organizations assess risk in

Term	Definition
	considering threats, vulnerabilities, likelihood, and consequences/impact; (iv) how organizations respond to risk once determined; and (v) how organizations monitor risk over time with changing mission/business needs, operating environments and supporting information systems. Example 1: The Facilities Department has an application that only runs on Windows XP, which is no longer supported. The system is attached to the network so technicians can also check email while using the application. The department plans to retire the application in two years. An alternative is available for $15,000. Using a risk-based approach, the system is removed from the network and the network port sealed. Another workstation is installed to allow email access for a cost of $1,000. The department addressed the risk and allocated resources appropriately. Example 2: The Financial Aid Department has consolidated all document storage, including tax returns and all financial aid functions, into a new hosted service. The department loaded the previous five years of data to support the current graduate and undergraduate population. This represents about 20,000 records, most of which contain one or more Social Security numbers. The presence of Social Security numbers and other personally identifiable information in large numbers means that a compromise of this system would result in significant harm and cost. Allocation of resources to invest in a full set of controls to protect the system and data is warranted according to a risk-based approach.

Term	Definition
Sanitization	A disposal process that renders Institutional Information on physical or logical media inaccessible at a certain level of effort. Various Sanitizing actions require increasing levels of effort to recover information. Note that Delete and Logical Delete are not Sanitization techniques. Example 1: Destroy, which makes retrieval fully impossible, is a Sanitization process. Example 2: Clear is a Sanitization process. Example 3: Purge is a Sanitization process. Example 4: Cryptographic Erase is a Sanitization process.
Security Event	See Information Security Event.
Separation of Duties	A process that addresses the potential for abuse of authorized privileges and helps reduce the risk of malicious activity without collusion. Separation of duties includes: (i) dividing operational functions and information system support functions among different individuals and/or roles; (ii) dividing information system support functions between different individuals (e.g., system management, programming, configuration management, quality assurance and testing, network security); (iii) ensuring that security personnel administering access control functions do not also administer audit functions. Example 1: The vendor payment application requires a voucher to be created by one user, the Purchasing Department to approve the voucher and the payables manager to approve the voucher before payment can be

Term	Definition
	issued. This example illustrates a separation of duties. Thanks to the separation of duties, it would require three distinct people to collude in order to conduct fraud. Example 2: The Student Health Services medical records application requires the user's manager to request access, and the department director and compliance office to approve. This example illustrates a separation of duties. No one person can request and approve access to medical records due to the separation of duties.
Service Provider	UC groups or organizations providing specific IT services to a Unit. Example 1: One Location provides managed computing resources and managed networking, which other Locations can use. Example 2: A central IT group at a UC campus provides computing resources or networking to Units. Example 3: An IT group in one Unit provides an application, such as a front desk sign-in system, to other Units.
Standard	1. A collection of specific and detailed requirements that must be met. 2. Requirements that specify the set of administrative, technical, or procedural controls necessary to meet the related policy. Standards differ from policy in that they can be more detailed and can change more rapidly in response to new technology or to new or evolving threats. Example 1: A set of security requirements to connect to a Location network is a Standard.

Term	Definition
	Example 2: A Data Classification Standard is another type of Standard. It provides specific guidance on how to classify Institutional Information using specific rules, examples, and samples of regulation to form a broad understanding of the different levels of Institutional Information.
Standard Change	1. A repetitive and identical change to a service or infrastructure with an approach that has been pre-authorized by the change management process. 2. A pre-authorized change that is low risk, common, and follows a pre-defined, repeatable procedure or work instruction to implement. Example 1: A password reset is a standard change. Example 2: Provisioning standard computing equipment to a new Workforce Member is a standard change. Example 3: A Location uses a particular networking switch in new installations and for all replacements. The deployment and installation processes are identical. The process has been proven over 10 previous installations and is now pre-approved for use as a standard change.
Standard Risk Treatment Plan	A pre-approved template of common controls to manage information security risk for a specific use case. Example 1: A Location has 38 offices that have various types of sign-in systems at their front desks. The CISO has approved a Standard Risk Treatment Plan that all 38 offices can implement to manage information security risk relating to their sign-in systems. The Units using these systems do not need to conduct a full Risk Assessment and can use the Standard Risk Treatment Plan for the set of security controls.

Term	Definition
	Example 2: A Location has more than 500 public-facing websites overseen by 25 Units. The CISO has approved a Standard Risk Treatment Plan for “public-facing websites with public data and no log-in requirements.” The 25 Units do not need to conduct a full Risk Assessment and can adopt the Standard Risk Treatment Plan if the criteria for its use are met.
Subject Matter Expert (SME)	Workforce Members who are responsible for their domain expertise. Example 1: Campus counsel is an SME on legal issues. Example 2: The CISO is an SME on information security issues. Example 3: The Registrar is an SME on student data.
Supplier	An external, third-party entity that provides goods or services to UC. These goods and services can include consulting services, hardware, integration services, software, systems, software-as-a-service (SaaS) and cloud services. Non-UC entities that operate IT Resources or handle Institutional Information are considered Suppliers for the purposes of this policy. A Vendor is a Supplier for the purposes of this policy. Example 1: A staffing firm that supplies consultants or temporary staff to perform job functions. Example 2: A software company that provides products and services to a Unit. Example 3: A local, value-added reseller that provides a range of products, installation services and consultants with specialized expertise.

Term	Definition
	Example 4: A cloud service vendor that offers one or more software applications.
Systemwide CISO	Systemwide chief information security officer who is responsible for security oversight throughout UC, such as protecting Institutional Information and IT Resources, assessing threats and vulnerabilities, leading incident management, developing security policy, educating staff regarding security, and reporting on security and risk to the UC president and appointed Regent committees. Example: The UC Office of the President CISO who reports to the UCOP CIO with systemwide scope and responsibility is a systemwide CISO.
UC Business	A broad term used to describe the activities related to operating the University of California. Example 1: Operating a Location library is UC Business. Example 2: Operating student housing constitutes UC Business. Example 3: Recruiting students to attend the university is also UC Business. Example 4: Submitting and processing grant applications is considered UC Business. Example 5: Providing medical care is UC Business. Example 6: Online learning is UC Business.
UC Network	A broad term intended to include all networks managed by UC. Example 1: A UC Network includes a wired network at the Location.

Term	Definition
	Example 2: A wireless network requiring UC managed authentication is a UC Network. Example 3: A non-public network provided by the Location is a UC Network. Example 4: A virtual private network (VPN) provided by the Location is a UC Network.
UC System/UC	1. A broad term intended to include all legal and operating entities managed by the Regents of the University of California. 2. A comprehensive reference to the entire University of California system, regardless of geographic location or function. 3. All University campuses, extension programs, and medical centers, the UC Office of the President, UC-managed national laboratories, and other University locations (campuses). Example 1: UC entities, such as medical centers, government affairs, non-USA offices, and campuses are part of the UC System. Example 2: Degree and non-degree granting campuses are part of the UC System. Example 3: UC Health System locations are part of the UC System. Example 4: Legislative offices in Sacramento, Calif., and Washington, D.C. are part of the UC System. Example 5: UC-managed laboratories are part of the UC System.

Term	Definition
	Example 6: UC Agricultural and Natural Resources is part of the UC System.
Unit	1. A point of accountability and responsibility that results from creating/collecting or managing/possessing Institutional Information or installing/managing IT Resources. A Unit is typically a defined organization or set of departments. 2. An IT, academic, research, administrative, or other entity operating within UC. 3. An academic school or administrative organization led by a Location appointed Unit Head. Example 1: Each of the following are Units when they budget, plan, and manage IT Resources for their organization: Housing, Student Health, Parking, Capital Planning, Admissions, Accounting, College of Biological Sciences, College of Letters and Science, School of the Arts and Architecture, School of Music, Police Department. Example 2: A vice chancellor of Student Affairs determines that all of its departments will budget for and plan IT Resources centrally. Thus, Student Affairs departments such as Housing, Dining, Admissions, Financial Aid, Student Health, and others form the Unit.
Unit Head	1. A general term for a dean, vice chancellor or person in a similarly senior role who has the authority to allocate budget and is responsible for Unit performance and administration. 2. At a specific Location or in a specific situation, people in the following senior roles may also be Unit Heads: department chairs,

Term	Definition
	assistant/associate vice chancellors (AVC), principal investigators, directors, senior directors, or senior managers. 3. A person in a senior management role with the authority to allocate budget and responsibility for Unit performance. Example 1: General managers in the Location Dining Operations Department report to an executive director, who reports to an AVC. The Unit Head is the AVC, unless the AVC specifically designates the executive director as the Unit Head for the purposes of this policy. Example 2: The dean of a Location’s medical school is the most senior executive. The dean is the Unit Head. Example 3: A faculty member is running a research project using IT Resources that they control/manage and the project involves faculty at other universities. The faculty member is the principal investigator and the Unit Head. Example 4: The university librarian reports to the chancellor and is responsible for the library’s budget, operations, and performance. The University Librarian is the Unit Head.
Unit Information Security Lead	A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities including, but not limited to: implementing security controls; reviewing and updating Risk Assessments and Risk Treatment Plans; devising procedures for the proper handling, storing and disposing of electronic media within the Unit; and reviewing access rights. These activities are performed in consultation with the Unit Head.

Term	Definition
	Example 1: The university librarian is a Unit Head. The librarian assigns to the library's director of IT the role of Unit Information Security Lead so that they will carry out the responsibilities of this policy. Example 2: The vice chancellor of Student Affairs is the Unit Head and assigns to the senior director of Technology Services the role of Unit Information Security Lead. Example 3: The dean of the School of Engineering is the Unit Head. The School of Engineering consists of seven departments, each of which has a computer resource manager. The dean assigns to each computer resource manager the role of Unit Information Security Lead for their department.
Utility Program	A program that performs a specific task, usually related to managing system resources. Operating systems contain several utilities for managing networks, users, disk drives, printers, and other devices. Utility programs can be found in several complex systems, such as developer tools, relational databases, and middleware. Developers often write small programs that help debug complex applications or automate tasks. These are considered utility programs. Example 1: The Microsoft Visual Studio development tool set, which is used by application developers, is a utility program. Example 2: The Oracle SQL Developer tool set, which is used by database administrators and application developers using the Oracle relational database platform, is a utility program.

Term	Definition
	Example 3: A small application that runs with elevated rights to delete temporary files because the main application does not always remove them is a utility program. Example 4: A script that looks for processes that are not responding and restarts them is a utility program.
Vendor	See Supplier.
Vital Records	Institutional Information essential for a Unit to continue business-critical functions, both during and after a disaster or emergency condition. (See also Business and Finance Bulletin, RMP-4.)
Workforce Manager	A person who supervises/manages other personnel or approves work or research on behalf of the University. Example 1: The general manager of a dining location supervises career and student workers (Workforce Members). The general manager is a Workforce Manager. Example 2: The assistant vice chancellor (AVC) of enrollment management supervises directors of admissions, financial aid, recruitment, registrar, and other support services. The AVC of enrollment management is a Workforce Manager. Example 3: The director of capital projects manages a staff of administrative and contract project-based Workforce Members. The director is a Workforce Manager. Example 4: A dean approves a principal investigator (PI) to hire staff and coordinate student volunteers to support a research project. The dean is

Term	Definition
	the Workforce Manager of the PI, and the PI is the Workforce Manager of the hired and volunteer staff. Example 5: Academic department administrative staff supporting faculty where the faulty member does not have a supervisor.
Workforce Member	An employee, faculty, staff, volunteer, contractor, researcher, student worker, student supporting/performing research, medical center staff/personnel, clinician, student intern, student volunteer, or person working for UC in any capacity or other augmentation to UC staffing levels. Example 1: An employee is a Workforce Member. Example 2: A student worker is a Workforce Member. Example 3: A registered volunteer is a Workforce Member. Example 4: A visiting researcher who is authorized to work at UC is a Workforce Member. Example 5: A temporary worker hired through a staffing firm is a Workforce Member. Example 6: A student or visiting student who trains or collaborates with other Workforce Members is a Workforce Member. Example 7: Unit Head is a Workforce Member. Example 8: Unit Information Security Lead is a Workforce Member.

Term	Definition
	Example 9: Medical, dental, pharmacy, nursing, and psychiatry students, trainees, and fellows attending a UC Health Location are Workforce Members.