University California - Systemwide IT Policy Glossary

Systemwide Review Draft

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 depends on a variety of factors, including role. For example, a Workforce Member's (employee's) acceptable use policy may differ from a student's. Example 1: The library offers complimentary wireless access to visitors. As part of the registration process, users review and agree to the terms that govern the use of this access, including not accessing or attempting to access UC IT Resources or facilities without proper authorization, or intentionally enabling 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 the terms that govern use of this access, including not running programs that attempt to calculate or guess passwords, or that are designed to trick users into disclosing their passwords.
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. Affiliation status for individuals other than UC students, faculty and staff must be authorized by the Unit and can include, but is not limited to, those in program, research, contract or license relationships with UC. Example 1: A visiting Ph.D. scholar is in residence at a Location to conduct independent research, and isn't receiving payment from UC.

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
	Example 2: A vendor, on site to conduct repairs, requires network access to run diagnostics and perform online troubleshooting.
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. 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.
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. HIPAA: The acquisition, access, use or disclosure of protected health information (PHI) in a manner not permitted under the HIPAA Privacy Rule.

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
	Example 1: Credit card numbers are harvested from a point of sale system. Example 2: Usernames and passwords are harvested from a campus server. Example 3: A USB drive is stolen, containing prospective and current students' names, addresses, incomes, phone numbers, high school GPA scores and Social Security numbers. Example 4: Electronic protected health information (PHI) is encrypted as the result of a ransomware attack.
CIO	Chief Information Officer. Senior executive responsible for information technology or information system functions throughout a Location. Example: IT Leadership Council member from a campus.
CISO	Chief Information Security Officer. A role responsible for security functions throughout a Location, including assisting in the interpretation and application of this policy. For some Locations, the appointment 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.

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
CRE	Cyber-risk Responsible Executive. A senior management position that 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: Provost. Example 2: Chief Financial Officer (CFO). Example 3: Chief Information Officer (CIO).
Critical IT Infrastructure	1. IT Resources that manage unrelated sets of Institutional Information or sets of very large or particularly sensitive Institutional Information. 2. IT Resources that meet two conditions: 1) A security “shared fate” among unrelated information systems is created via a dependency on the IT Resource; and 2) The default control set approach (a standard method for securing a system) is inappropriate given the risk, complexity or specialized nature of the IT Resource. Example 1: Active Directory, which maintains information about users, permissions and other security-related attributes. Example 2: A single departmental server performing many critical functions. The combination of these functions results in a system that requires special security measures. Example 3: Encryption key management system. Example 4: Firewall protecting Electronic Medical Record (EMR) system databases.

Term	Definition
	Example 5: Domain Name System outside of central IT. Example 6: Wired and wireless networking equipment that provides access to Institutional Information protected by regulation or contract (health information or credit card track data, for example).
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 this business. Documentation and reviews are produced after the change. Example 1: A vendor requires the application of a patch to resolve a major outage. Example 2: A critical application is down, and the technical team requires the installation of a diagnostic tool to troubleshoot the problem.
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.
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. The 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.

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
Guideline	A collection of system-or procedure-specific recommendations for best practices. Guidelines are strongly recommended practices or steps, but they aren't required. Example 1: The Microsoft Windows hardening guide. Example 2: A vendor's best practice guide for securing a system.
Incident	See Information Security Incident.
Information Security Event Security Event	1. An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security-relevant. 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. Example 2: Firewall log monitoring software logs remote connection attempts from an unexpected location. Example 3: Windows log monitoring records the creation of a new local administrator account on a point-of-sale terminal. Example 4: A user finds and exploits a bug that allows a re-do of a transaction that should be locked.
Information Security	A compromise of the confidentiality, integrity or availability of

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
Incident Security Incident	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. Example 2: An attacker prevents the medical record system from functioning for patients and practitioners. Example 3: An attacker takes personnel data from a payroll system. (Note: This is also an example of a Breach.)
Institutional Information	A term that broadly describes all data and information created, received and collected by UC. Example 1: Information contained in a database, such as employee personnel records or records pertaining to student enrollment and grades. Example 2: Activity log data from a server application or network device. Example 3: Emails sent and received pertaining to UC business. Example 4: Instrument measurements from academic research, collected manually or electronically. Example 5: Electrical use data collected by a building automation system.
Institutional	See Proprietor.

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
Information 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. Example 3: A storage device crashes and leaves files corrupted, causing a loss of integrity. A back-up is used to restore the file. 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, maintaining 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 that data by allowing only authorized users to make changes.
ISMP	Information Security Management Program. 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 cybersecurity to manage risk to acceptable levels. This includes management commitment, policies, standards, procedures, work instructions, tools,

Term	Definition
	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. Example 2: Student Affairs IT creates and documents a program explaining policies, work instructions, risk management, tools, conventions, training, personnel requirements and contractual requirements.
ISO	Information Security Officer. See CISO.
ISO 27000/International Organization for Standardization 27000	A collection of information security guidelines intended to help an organization implement, maintain and improve its information security management. Example 1: ISO 27002:2103 is a comprehensive set of controls focused on information security. Example 2: ISO 27005:2103 is focused on information security risk management.
IT Resource(s)	A term that broadly describes resources with computing and networking capabilities. These include, but are not limited to: personal and mobile computing devices, mobile phones, printers, network devices, industrial control systems (SCADA), access control systems, digital video monitoring systems, data storage systems, data processing systems, backup systems, electronic and physical media, biometric and access tokens, and other devices that connect to any UC network. This includes both UC-owned and personally owned devices.

Term	Definition
	Example 1: A Cisco firewall installed in a data center or building communications room. Example 2: An electrical and temperature monitoring system used for a building's LEEDS certification. Example 3: A video camera surveillance system. Example 4: A database server. Example 5: A network-attached printer, scanner and copier. Example 6: A computer, including a laptop, server or point-of-sale system. Example 7: A personal smartphone used to access email and manage a calendar. Example 8: A personal PC used to work remotely on UC business. Example 9: Personally owned computers, tablets or other devices connected to non-public campus networks or used to process, store or transmit Institutional Information.
IT Workforce Member	A Workforce Member who is assigned specific Information Technology 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: The school of business employs a multimedia technician. Role responsibilities also include PC and equipment installation, patching, software installation and event support. Since the role

Term	Definition
	includes IT duties, the technician also has the additional responsibilities of IT Workforce Member. 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 also has the additional responsibilities of IT Workforce Member. Example 4: The central IT group has a group of database administrators. Since the role includes IT duties, the administrators also have the additional responsibilities of IT Workforce Members.
Least Privilege Access	The practice of limiting access to the minimum level that will allow normal functioning. Applied to employees, this principle translates to giving people the lowest level of access rights that they require to do their jobs. Applied to security architecture, each entity is granted the minimum system resources and authorizations that 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. The cashier does not need access to the register's operating system or its administrative functions. Example 2: A financial analyst runs a monthly vacation and leave report for department managers. Someone else developed the report. 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 the local machine for a file. The directory permissions can be set granularly. 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. The attendant can read, but not update, the records. Read access is all that's required for this specific role.
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 in the United States controlled by the Regents of the University of California. Example 1: A specific UC campus. Example 2: A geographically separated office such as the UCPath 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. Example 4: The San Diego Supercomputer Center, an Organized Research Unit of the University of California, San Diego.
Need-to-Know	1. A method of isolating information resources that a user requires to do his/her job, but no more than that. 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.

Term	Definition
	HIPAA refers to this as “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. In FERPA a legitimate educational interest is necessary for a Workforce Member to carry out his/her responsibilities in support of UC's educational mission. Think of legitimate educational interest as 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. 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. Go-live is scheduled in two weeks. All testing and documentation is complete, or will be by then. The project manager completes the change request and supplies all the documentation for approval. The code and security reviews are

Term	Definition
	complete. There is a roll-back plan. Example 2: A Location's Facilities department has scheduled a vendor to replace 25 video cameras in parking garages and near parking pay-stations. The maintenance manager completes the change request, and the vendor provides all the supporting documentation for the installations starting next week. The network and storage teams completed their reviews last week. 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. 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.
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. Example 2: The detailed steps required to grant a new employee access to the network and systems.
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

Term	Definition
	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. 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 is appropriately approved by the Registrar to obtain an SIS extract of students who are taking a series of science, technology, engineering and math classes. The Department of Chemical and Environmental Engineering later asks the Math Department for the data for a similar analysis. 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

Term	Definition
	the request and 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 Advancement, and the Proprietor for student data related to graduation, majors and GPA is the Registrar. Therefore, the Executive Director of 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 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.
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 (Level 1) to the highest level of 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 (Level 1). Integrity concerns do exist, however, so appropriate protection must be in place.

University California - Systemwide IT Policy Glossary
Systemwide Review Draft

Term	Definition
	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 (Level 4). Example 3: A researcher is collecting human subject data. The data set initially contains personally identifiable information. The researcher plans to later de-identify the data. Until the data is fully de-identified, it will require the highest level of protection (Level 4) due to statutory requirements for protecting specific types of personal information. Example 4: A researcher receives a large, multi-year 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.
Researcher	A UC faculty member conducting research on behalf of UC. Also a Workforce Member. Example 1: Principal Investigator or other designation paid by UC. Example 2: Research collaborators at other institutions who are creating, securing and maintaining Institutional Information. Example 3: Staff research assistants. Example 4: Graduate student who is performing research and is creating, securing and maintaining Institutional Information.
Risk Assessment	A process to identify, rate and prioritize risk, as well as to document risk tolerance. Example 1: As part of its risk management process, a department identifies the likelihood and impact of specific harmful events and

Term	Definition
	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 visibility to risks and assist management in making decisions. Tabs in the spreadsheet guide the process and ask relevant questions. Example 2: A Location adopts an IT governance, risk management and compliance (GRC) tool. The GRC tool has workflows and risk rating systems to help identify, prioritize and manage information security risks.
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 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.

Term	Definition
	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.
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 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 Unit 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

Term	Definition
	each installation.
Security Event Information Security Event	1. An identified occurrence of a system, service or network state indicating a possible breach of information security policy or failure of controls, or a previously unknown situation that may be security-relevant. 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 a Security Incident (see definition below). Example 1: Antivirus software sends an alert when malware is detected. Example 2: Firewall log monitoring software logs remote connection attempts from an unexpected location. Example 3: Windows log monitoring records the creation of a new local administrator account on a point-of-sale terminal. Example 4: A user finds and exploits a bug that allows a re-do of a transaction that should be locked.
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, and network security);

Term	Definition
	(iii) ensuring 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, and the payables manager to approve before payment can be issued. This example illustrates a separation of duties. It would require three distinct people to collude 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.
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. Specifies the minimum set of administrative, technical or procedural controls required to meet the related policy. Standards will often change more rapidly than policy in response to new technology and new or evolving threats.

Term	Definition
	Example 1: Minimum security standards to connect to a Location network. Example 2: Data Classification Standard, a document that 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 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, relatively common, and follows a pre-defined, repeatable procedure or work instruction to implement. Example 1: A password reset. Example 2: Provision of standard equipment to a new Workforce Member. Example 3: A Location uses a particular switch as a standard in new installations and replacement. The deployment and installation processes are identical. The process has been proven over 18 previous installations and is now pre-approved for use.
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 some form of sign-in system at the front desk. 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

Term	Definition
	and can adopt the Standard Risk Treatment Plan if the criteria for its use are met. Example 2: A Location has more than 500 public-facing websites. Currently 38 Units oversee the websites. The CISO has approved a Standard Risk Treatment Plan for "public-facing websites with public data and no log-in requirements." The 38 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.
Supplier	An external, third-party entity that provides goods or services. These goods and services can include consulting services, hardware, integration services, software, systems, software as a service (SaaS) and cloud services. Non-UC entities Those who 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. Example 4: A cloud service vendor that offers one or more software applications.
Systemwide CISO	Systemwide Chief Information Security Officer. Responsible for security oversight throughout UC, such as protecting Institutional

University California - Systemwide IT Policy Glossary

Systemwide Review Draft

Term	Definition
	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: UC Office of the President CISO who reports to the UCOP CIO with systemwide scope and responsibility.
UC Network	A broad term intended to include all networks managed by UC. Example 1: A wired network at the Location. Example 2: A wireless network requiring authentication. Example 3: A non-public network provided by the Location. Example 4: A virtual private network (VPN) provided by the Location.
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 and medical centers, the UC Office of the President, UC-managed national laboratories and other University locations (campuses). Example 1: UC entities, such as UC-managed laboratories or medical centers, government affairs offices and campuses. Example 2: Degree and non-degree granting campuses. Example 3: UC Health System locations.

Term	Definition
	Example 4: Legislative offices in Sacramento, Calif., and Washington, D.C. Example 5: UC-managed laboratories.
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. IT, academic, research, administrative or other entity operating within UC. This should be interpreted broadly to include all computing systems, network-attached devices (IT Resources) and data (Institutional Information). 3. An academic school or administrative organization headed by a 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 student affairs departments will budget for and plan IT Resources centrally. Thus, student affairs departments like Housing, Dining, Admissions, Financial Aid, Student Health and others become the Unit. **Special Note**: Information security risk management is a fundamental business concern, in the same way that fiscal planning and financial management are fundamental business concerns.

University California - Systemwide IT Policy Glossary
Systemwide Review Draft

Term	Definition
	Information security risk management must be considered alongside all other Unit activities to enable proper resourcing and prioritization.
Unit Head	1. A generic term for Dean, Vice Chancellor or similarly senior role who has the authority to allocate budget and is responsible for Unit performance. 2. A senior management role with the authority to allocate budget and responsibility for Unit performance. 3. At a specific location or in a specific situation the following senior roles may also be Unit Heads: department chairs, assistant/associate vice chancellor (AVC), principal investigators, directors, senior directors or senior managers. 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 top executive. The dean is the Unit Head. Example 3: A faculty member is running a large research project under a federal grant that 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 the Unit Head.
Unit Information Security Lead	A term for the Workforce Member(s) assigned responsibility for tactical execution of information security activities associated with this policy. Activities include, but are not limited to: implementing security

Term	Definition
	controls; reviewing and updating Risk Assessment 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. Example 1: The University Librarian is a Unit Head. The Librarian names the library's Director of IT as the Unit Information Security Lead to carry out the responsibilities of this policy. Example 2: The Vice Chancellor of Student Affairs is the Unit Head and assigns 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 each Computer Resource Manager the role of Unit Information Security Lead for his/her 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.

Term	Definition
	Example 2: The Oracle SQL Developer tool set, which is used by database administrators and application developers using the Oracle relational database platform. Example 3: A developer writes a small application to run with elevated rights to delete temporary files because the main application does not always remove them. Example 4: A developer writes a script that looks for processes that aren't responding and restarts them.
Vendor	See Supplier.
Workforce Manager	Person who supervises/manages other personnel or approve 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 staff. The director is a Workforce Manager. Example 4: A dean approves a principal investigator (PI)/researcher to hire staff and coordinate student volunteers to support a research project. The dean is the Workforce Manager of the PI, and the PI is the Workforce Manager of the hired and volunteer staff.
Workforce Member	Employee, faculty, staff, volunteer, contractor, researcher, student

Term	Definition
	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. Example 2: A student worker. Example 3: A registered volunteer. Example 4: A visiting researcher who is authorized to work at UC. Example 5: A temporary worker hired through a staffing firm. Example 6: A student or visiting student who trains or collaborates with other Workforce Members. Example 7: Unit Head. Example 8: Unit Information Security Lead.