

Term	Definition
Anti-virus Software	Software that detects or prevents malicious software.
Application	A software program designed to perform a specific function for a user. Applications include, but are not limited to, word processors, database programs, development tools, image editing programs, and communication programs.
Authentication	The process of confirming that a known individual is correctly associated with a given electronic credential; for example, by use of passwords to confirm correct association with a user or account name (is a term that is also used to verify the identity of network nodes, programs, or messages).
Authorized	The process of determining whether or not an identified individual or class has been granted access rights to an information resource, and determining what type of access is allowed; e.g., read-only, create, delete, and/or modify.
Availability	Ensuring that information assets are available and ready for use when they are needed.
Campus	A “campus” is any CSU campus and the Chancellor’s Office.
Campus Limited Access Area	Physical area such as a human resources office, datacenter, or Network Operations Center (NOC) that has a defined security perimeter such as a card controlled entry door or a staffed reception desk.
Campus Managers	Responsible for (1) specifying and monitoring the integrity and security of information assets and the use of those assets within their areas of program responsibility and (2) ensuring that program staff and other users of the information asset are informed of and carry out information security and privacy responsibilities.
Catastrophic Event	An event that causes substantial harm or damage to significant CSU information systems, network resources, or data. Examples: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.
Confidentiality	The need for protection of data from unauthorized disclosure.
Control	Countermeasures (administrative, physical, and technical) used to manage risks.
Critical Asset	An asset that is so important to the campus that its loss or unavailability is unacceptable.

Term	Definition
CSU Network	Any CSU administratively-controlled communications network that is within the CSU managed physical space. Such networks may interconnect with other networks or contain sub networks.
Data	Information systems, data (information in electronic or non-electronic such as in paper format or stored/captured audio communication), and network resources.
Data Owner	Person identified by law, contract, or policy with responsibility for granting access to and ensuring appropriate controls are in place to protect information assets.
Data Stewards (also known as “Data Custodian”)	Persons with operational responsibility for the physical and electronic security of the data.
DMZ	A network inserted as a “neutral zone”.
Electronic Media	Includes, but is not limited to, floppy disks, backup tapes, CD-ROMs, zip drives, flash drives, memory sticks, and portable hard drives.
Employee	Any person who is hired by the CSU to provide services to or on behalf of the CSU and who does not provide these services as part of an independent business.
Excessive Authority	Assignment of a single individual to overlapping administrative or management job functions for a critical information asset without appropriate compensating controls such as added reviews or logging.
Hardening	A defensive strategy to protect against attacks by removing vulnerable and unnecessary services, patching security holes, and securing access controls.
Hardware	Includes, but is not limited to, portable and non-portable workstations, laptops, servers, copiers, printers, faxes, and PDAs.
Information Security Program	An organizational effort that includes, but is not limited to: security policies, standards, procedures, and guidelines plus administrative, physical, and technical controls. The effort may be implemented in either a centralized or a decentralized manner.
Information Assets	Information systems, data, and network resources to include automated files and databases.
Information Systems	Systems that include, but are not limited to laptop computers, workstations, servers, and mobile devices.
Integrity	The accuracy, completeness, and validity of information.

Term	Definition
Least Privilege	A concept of information security by which users and their associated applications execute with the minimum amount of access required to perform their assigned duty or task.
Logical Access	The connection of one device or system to another through the use of software.
Malicious Software	Software designed to damage or disrupt information assets.
Mobile Devices	Devices containing electronic CSU data which are easily transported. Such devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), and “smart” phones.
Need-to-Know	A concept of information security by which data is only provided to users who require the information to perform an assigned duty or task.
Network Resources	Resources that include, but are not limited to: network devices (such as routers and switches), communication links, and network bandwidth.
Non-public	All services except those services intended for public access and use.
Notice-triggering Information	Specific items of personal information identified in California Civil Code Sections 1798.29 and 1798.3.
Personally Identifiable Information	Information which can potentially be used to uniquely identify, contact, or locate a single person.
Physical Access	Being able to physically touch, use, and interact with information systems and network devices.
Private IP Addresses	Defined in RFC 1918 as 10.0.0.0/8; 172.16.0.0/12, and 192.168.0.0/16.
Protected Data	Level 1 and Level 2 data which are defined in the CSU Data Classification Standard. This data has been categorized according to its risk to loss or harm from disclosure.
Public Information	Any information prepared, owned, used or retained by a campus and not specifically exempt from disclosure requirements of the California Public Records Act (Government Code Sections 6250-6265) or other applicable state or federal laws.
Remote Access	Any connection from an external, non-campus network to any campus information system, data, or network resource.
Risk	The likelihood of a given threat exercising a particular potential vulnerability, and the resulting impact of that adverse event on an organization.

Term	Definition
Risk Assessment	A process by which quantitatively and/or qualitatively, risks are identified and the impacts of those risks are determined. The initial step of risk management.
Risk Management	A structured process which identifies risks, prioritizes them, and then manages them to appropriate and reasonable levels.
Security Awareness	Awareness of security and controls, in non-technical terms, conveyed to motivate and educate users about important security protections that they can either directly control or be subjected to.
Security Incident	<p>An event that results in any of the following:</p> <ul style="list-style-type: none"> • Unauthorized access or modification to the CSU information assets. • An intentional denial of authorized access to the CSU information assets. • Inappropriate use of the CSU's information systems or network resources. • Inappropriate disclosure of CSU data.
Security Training	Specific technical understanding of how to secure the confidentiality, integrity, and availability of information systems (including operating systems and applications), networks, and data to prevent or detect security incidents.
System Administrator (also known as "System Personnel" or "Service Providers")	Individuals who manage, operate, and support campus information systems or networks.
Third Parties	Include, but are not limited to, contractors, service providers, vendors, and auxiliaries, and those with special contractual agreements or proposals of understanding.
Threat	A person or agent that can cause harm to an organization or its resources. The agent may include other individuals or software (e.g. worms, viruses) acting on behalf of the original attacker.
User	<ul style="list-style-type: none"> • Anyone or any system which accesses the CSU information assets. • Individuals who need and use University data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust and as such are responsible for protecting the security and integrity of those data.
User Information	Information which can be used to uniquely identify, contact, or locate a user.
Vulnerability	A flaw within an environment which can be exploited to cause harm.
Vetting	Formal and thorough examination (usually by stakeholders and/or subject matter experts) prior to grant of approval or clearance.