ICSUAM Policy Glossary

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 assets, 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.

Biometric Devices – An instrument intended to validate the identity of an individual through comparison of a demonstrated intrinsic physical or behavioral trait with a record of the same information previously captured. Examples: fingerprint, retina scan, voice recognition.

Business Continuity Planning - See CSU BCP Executive Order.

Campus - For the purposes of the CSU Security Program, a "campus" is any CSU campus as defined in Section 89001 of the California Education Code to include satellite locations and the Chancellor's Office.

Campus Limited Access Area - Physical area such as a human resources office, data center, 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 assets. Examples: earthquake, fire, extended power outage, equipment failure, or a significant computer virus outbreak.

Computer Security Incident Response Team (CSIRT) - The name given to the team that handles security incidents.

Confidentiality - Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C, SEC. 3542]

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.

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 - Individual facts, statistics, or items of information represented in either electronic or non-electronic forms.

Data Center - A facility used to house information processing or telecommunications equipment that handle protected or critical information assets.

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. The duties include but are not limited to classifying, defining controls, authorizing access, monitoring compliance with CSU/campus security policies and standards, and identifying the level of acceptable risk for the information asset. A Data Owner is usually a member of management, in charge of a specific business unit, and is ultimately responsible for the protection and use of information within that unit.

Data Steward - (also known as "Data Custodian") An individual who is responsible for the maintenance and protection of the data. The duties include but are not limited to performing regular backups of the data, implementing security mechanisms, periodically validating the integrity of the data, restoring data from backup media, and fulfilling the requirements specified in CSU/campus security policies and standards.

DMZ – DMZ (De-Militarized Zone) is a set of one or more information assets logically located outside of a protected network that is accessible from the Internet (open to the world) with limited controlled data exchanges with the protected environment.

Electronic Media - Electronic or optical data storage media or devices that include, but are not limited to, the following: magnetic disks, CDs, DVDs, flash drives, memory sticks, and tapes.

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.

Encrypted Protocol - An agreed-to secure means of data transmission over a network (wired or wireless).

Encryption - The process of encoding data so only the sender and the intended recipient can read it.

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 - Physical devices including, but is not limited to, portable and non-portable workstations, laptops, servers, copiers, printers, faxes, and PDAs.

Information Assets - Information systems, data, and network resources to include automated files and databases.

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 Systems - A combination of hardware, network and other resources that are used to support applications and/or to process, transmit and store data.

Integrity - Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]

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.

Lockout Time - The amount of time for which logins to an account are disabled. Usually invoked once a threshold of invalid login attempts has been reached.

Logical Access - The connection of one device or system to another through the use of software.

Malicious Software - Software designed to damage or disrupts information assets.

Mobile Devices - Devices containing electronic CSU data that are easily transported. Such devices include, but are not limited to: laptop computers, personal digital assistants (PDAs), and “smart” phones.

Network Resources - Resources that include, but are not limited to: network devices (such as routers and switches), communication links, and network bandwidth.

Non-public - A service or information intended only for the internal use of the organization.

Notice-triggering Information - Specific items of personal information identified in California Civil Code Sections 1798.29 and 1798.3.

Operating System - Software that is primarily or entirely concerned with controlling a computer and its associated hardware, rather than with processing work for users.

Patch (Patching) - The installation of a software update designed to fix problems, improve usability, or enhance performance.

Personally Identifiable Information - Any information that identifies or describes an individual, including, but not limited to name, Social Security number, physical description, address, phone number, financial matters, medical or employment history (California Information Practices Act).

Physical Access - Being able to physically touch, use, and interact with information systems and network devices.

Private IP Addresses - Defined by Request for Comment (RFC) 1918 as range of non-routable addresses.

Protected Asset - Information asset containing protected data.

Protected Data - Level 1 and Level 2 data that 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.

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 that identifies risks, prioritizes them, and then manages them to appropriate and reasonable levels.

Risk Mitigation - Reduce the adverse effect of an event by reducing the probability of the event occurring and/or limiting the impact of the event if it does occur

Screen Filter - An item that can be used to limit the visibility of content displayed on a computer screen to those who are immediately in front of it.

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 - An event that results in any of the following: 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. The attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations.

Security Training - Specific technical understanding of how to secure the confidentiality, integrity and availability of applications, operating systems and information assets to prevent or detect security incidents

System Administrator - (also known as "System Personnel" or "Service Providers") Individuals, who manage, operate, support campus information systems; or manage networks.

Third Parties - For the purposes of the CSU Security Program, third parties include, but are not limited to, contractors, service providers, vendors, 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 - Anyone or any system that 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.

Vulnerability - A flaw within an environment that can be exploited to cause harm.