Information Security Policies Terms & Glossary

DOCUMENT CONTROL

DOCUMENT NAME: Information Security Policies Terms & Glossary

DOCUMENT ID REFERENCE: Reference 01

AUTHORIZATION:

Prepared By	Reviewed By	Approved By
IS GRC Staff	Sandra Taylor	Gus Anagnos
	Director of IS GRC	CISO
Date: 04/05/2019	Date: 04/30/2019	Date: 05/03/2019

VERSION HISTORY:

Version	Issue Date	Effective Date	Prepared By	Authorized By	Description
1.3	09/01/2021		Information Security Governance, Risk Management & Compliance		• Updated definitions
1.2	11/01/2019		Information Security Governance, Risk Management & Compliance		• Updated definitions
1.1	09/01/2019		Information Security Governance, Risk & Compliance	Gus Anagnos	• Updated definitions • Updated grammar and typo edits
1.0	05/03/2019		Information Security Governance, Risk & Compliance	Gus Anagnos	Original Version

Term	Definition
Academic Need	An academic need accomplishes a scholarly purpose, including but not limited to grant-supported research, academic assignments, and any activities required to complete USC coursework.
All Staff and Other Employees	All university faculty members (including part time and visiting faculty), staff and other employees (such as postdoctoral scholars), and students (including postdoctoral fellows and graduate students) as well as any other users of the network infrastructure, including independent contractors or others (e.g., temporary agency employees) who may be given access on a temporary basis to university systems
Asset Custodian	All IT assets are wholly owned by USC, but the Asset Manager is the person primarily responsible for the asset. This is traditionally the individual who procured and/or provisioned the asset, or the person for which the asset was procured for
Asset User	The person in possession of the asset or executing the function of the asset. This person may have been provisioned an asset by the Asset Custodian, who is ultimately responsible for the asset. All IT assets are wholly owned by USC
AUP	Acceptable Use Policy
Authentication	Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system
Availability	Authorized users have access to the systems and the resources they need
Back-Out Plan	The back-out plan is developed in parallel with the implementation plan and outlines the steps to be followed to back-out of a change implementation, as well as the conditions that should exist in order for the back-out to be invoked. The complexity of a back-out plan depends on the type and complexity of the change. For routine changes, a standard back-out plan may be available. However, the extent to which these are be utilized should be determined on a case-by-case basis
Business Associates Agreement (BAA)	A legal document between a healthcare provider and a contractor, when that vendor might receive access to Protected Health Information (PHI)
Business Need	A business need accomplishes a financial or other legitimate operational purpose, including but not limited to payroll, human resources, operations, and other business management functions
Change	A change is any adjustment or modification to any hardware, system software, application software, or system component within the development, production and test environments, including parameters tables, but excluding those items that would fall under daily operations (patient, provider table record updates)

Cloud Services	A paradigm for enabling on-demand network access to a shared pool of physical and virtual computing resources (e.g. networks, servers, storage, applications, and services) that support self-service provisioning and management. Division of management responsibilities between the customer and provider vary by service model
Confidential	Data that typically includes regulated data requiring compliance efforts if exposed to unauthorized parties, or would cause legal, financial, reputational, operational harm if disclosed
Confidential-Controlled Data	Data that is a sub-category of Confidential and is to be used only for Covered Defense Information, which includes Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), or any other information that has military or space application where the data provider (e.g. research sponsor) has imposed safeguarding or dissemination controls for reasons of national security.
Confidentiality	Data, objects and resources are protected from unauthorized viewing and other access
Covered Individuals	People or entities specified by the scope of a policy
Dark Web	A hidden network of servers and websites that requires special software to access. The dark web, also known as darknet, provides anonymous access to the internet for people who want to keep information about themselves hidden from view. It also provides anonymous hosting
Data Security Addendum (DSA)	A legal document used during the procurement process that is designed to protect and limit the unauthorized disclosure and use of personal information and proprietary technical data between a vendor and USC
Electronic Media	Electronic media (i.e., “soft copy”) are devices that contain memory storage such as hard drives, random access memory (RAM), read-only memory (ROM), discs, and flash memory. Equipment that contain such devices including; phones, mobile computing devices, networking devices, and any additional type of device that stores information
Encryption	The process of encoding a message or information in such a way that only authorized parties can read it
Endpoint Security	A subset of cybersecurity that protects networked devices, such as smartphones and medical equipment, that are usually accessed by an individual user or group
Firewall	A network security system built into hardware or software that monitors network traffic and controls incoming and outgoing traffic based on a set of rules
Hard Copy Media	Hard copy media are physical representations of information, most often associated with paper printouts

Hardening	The act or process of making a network, data repository, sensor, computer system, software, or other equipment resistant to unauthorized access or damage
High Value Asset (HVA)	USC information systems that create, process, transmit or store High Value Information (HVI)
High Value Information (HVI)	Data that if inappropriately disclosed, accessed, used, disrupted, modified or destroyed, could cause significant impact, as defined by the Information Risk Standard, to USC's reputation and public confidence. High Value Information (HVI) could be Confidential, Internal Use, or Public data
Identity and Access Management (IAM)	Identity and Access Management - The information security discipline that establishes roles and manages the requests for access to information and related information processing services; Identity management enables companies to control who, how, when, and which users access information, digital assets or specific physical facilities
Incident Response Plan	A systematic and documented method of approaching and managing situations resulting from IT security incidents or breaches
Information Owner	Individual or Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal
Information Security (InfoSec)	Information security - protecting against the unauthorized use of information, especially electronic data, or the measures taken to achieve this
Information Security Risk Assessments	A systematic process of identifying and evaluating potential risks that may exist in a given environment (or for a system) in order to prioritize for risk mitigation
Integrity	Data is protected from unauthorized changes to ensure that it is reliable and correct
Internal Use Only	Data that includes all information used to conduct USC business, unless categorized as "Confidential" or "Public"
Internet Services	Access to internet provided by USC
Intrusion Detection System (IDS)	A system that can execute logging and monitoring to discover unauthorized system modifications
Intrusion Prevention System (IPS)	A network security/threat prevention technology that examines network traffic flows to detect and prevent malicious inputs to a target application or service that attackers use to interrupt and gain control of an application or machine
IS GRC (Information Security Governance, Risk Management, Compliance)	A combination of three approaches that organizations use to demonstrate compliance with international standards, global rules, laws, and state regulations. Governance, risk management,

	compliance (GRC) is often implemented by companies that are growing globally to maintain consistent policies, processes, and procedures across all parts of the organization
ITS	Information Technology Services
Junk Email	Unwanted or unsolicited email, typically in the form of advertising or promotional material
Least Privilege Access	A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions
Local Technology Support	Information technology support dedicated within a local school or unit
Major Configuration Changes	An adjustment or modification to any production hardware, system software, application software, or system component that would have a negative impact on critical or key systems and the daily operations of a school, unit or the broader USC environment (i.e. version change, software update, operation system update). This would exclude those items that would fall under daily operations
Major Significance	A system is considered of major significance if it impacts the daily operations of a unit or school
Network Infrastructure Use (NIU)	The University of Southern California provides its faculty, staff and students with a network infrastructure to facilitate the missions of the university, including instruction, research, service and administration. The purpose of this policy is to confirm the ownership of the USC Network Infrastructure, defined below, and establish the responsibilities of faculty, staff, students and other employees in protecting and securing the network infrastructure
Network Owner	The person or entity responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of a network
Network Services	A capability that facilitates a network operation, such as WIFI, Voice over IP (VOIP), Local Area Networks, etc.
OCISO	Office of the Chief Information Security Officer
Personal Devices	Refers to devices, such as a laptop, tablet or smartphone owned by an individual, and not owned, reimbursed or paid for by USC
Personally Identifiable Information (PII)	Any data that could potentially identify a specific individual
Phishing	An exploit in which an attacker, typically using email, attempts to trick a computer user into opening web links, entering personal information into a web form or fake website, or taking an action that allows the attacker to obtain sensitive information. Spear phishing targets a specific individual or group of individuals using personal information
Privileged Access	A user or information system account that is authorized (and, therefore, trusted) to perform security relevant functions that ordinary users are not authorized to perform.

	• This consists of the following;
	  ○ Administrative access to systems or data (e.g., server or database administrators)
	  ○ Access to systems and resources beyond standard user levels and permissions
	  ○ Ability to modify security settings, create users, and grant access
	  ○ Ability to bypass or circumvent security controls

Protected Health Information (PHI)	Also referred to as personal health information, generally refers to demographic information, medical histories, test and laboratory results, mental health conditions, insurance information, and other data that a healthcare professional collects to identify an individual and determine appropriate care
Public	Data that is not regulated and is generally made available through public interfaces and requires no protection mechanisms
Ransomware	Malicious code that encrypts files on a computing device, enabling an attacker to demand a ransom from the legitimate owner to recover the encrypted data
Reasonable Level	The standard USC Risk Leadership deems appropriate for the specific information risk
Security by Design Objective	System designed from the foundation to be secure
Security Incident	Any information security event which has the potential to or has already resulted in unauthorized access, acquisition, manipulation, or destruction of data which compromises the Confidentiality, Integrity or Availability of university information assets, including those which may be handled, stored, or accessed by third party services, products or related processes
Separation of Duties	A security principle that divides critical functions among different staff members to ensure that no one individual has enough information or access privilege to perpetrate damaging fraud or misuse systems
Service Level Agreement (SLA)	A service level agreement (SLA) is a contract between a service provider and the customer that defines the level of service expected from the service provider. SLAs are output-based in that their purpose is specifically to define what the customer will receive. SLAs do not define how the service itself is provided or delivered. Though each SLA may vary depending on the service provider, the areas covered are consistent across SLAs, including responsiveness, work volume, quality, precision, accuracy, and speed
Singled Sign-On (SSO)	Enables users to leverage the same username and password across multiple networks. This capability might also allow users to use the same credentials across different systems

Social Engineering	A human-centric manipulation technique that uses deceptive tactics to trigger emotionally driven actions that are in the interests of a cybercriminal or attacker
SVP	Senior Vice President
System Development Lifecycle	A process for planning, creating, testing, and deploying an information system
System Owner	The individual responsible for the overall procurement, development, integration, modification, operation, maintenance, and retirement of an information system. The System Owner is a key contributor in developing system design specifications to ensure the security and user operational needs are documented, tested, and implemented
Third Party	Any outside individual or entity who is not a university student, faculty or staff employee who contractually interacts with or on behalf of USC. This includes but is not limited to vendors, consultants, contractors, and research and business partners
Third Party Relationship Owner	The individual responsible for establishing and managing the interactions between a third party and USC
USC	University of Southern California
USC Board of Trustees	An appointed or elected group of individuals that has overall responsibility for the management of an organization
USC-Distributed	Infrastructure, licensing or devices provided by USC
USC Information Risk Governing Bodies	USC risk governance bodies established by USC Risk Management Leadership
USC-Owned	Asset owned, reimbursed or paid for by University of Southern California
USC-Owned Technology Resources	USC network-based communication services and file repositories (including but not limited to, USC networks, USC email accounts, USC instant message, and USC cloud-based repositories); USC-issued computers and electronic devices (including but not limited to, desktops, laptops, servers, mobile phones, tablets, PDAs, and pagers) that are purchased or leased using university funds; and USC purchased, licensed, or developed software
USC Risk Management Leadership	USC Risk Management leadership is defined as chartered and approved information risk governance bodies
USC Confidential information	Data that is not classified as "confidential" by government regulations, but that is confidential to members of the USC community. Data of this type cannot be shared publicly with external users, outside entities, or members of the media without express approval from relevant USC authorities