FSU | INFORMATION TECHNOLOGY SERVICES

IT GLOSSARY

Alphabetical list of terms and definitions for words and titles used throughout IT standards

---

2-Factor Authentication (2FA) – a subset of Multi-Factor Authentication (MFA). 2FA is a security enhancement that requires two pieces of evidence (your credentials) when logging in to an account. Credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Credentials must come from two different categories to enhance security.

Access Control - the practice of authorizing and granting appropriate access and privileges to legitimate users for resources, transactions, functions, and activities.

Access Point – any piece of equipment that allows wireless communication using transmitters and receivers to communicate. These devices act as hubs and enable communications to the campus network.

Administrative Account - a user account with elevated privileges on a device. Such an account is intended to be used only when performing personal computer (PC) management tasks, such as installing updates and application software, managing user accounts, and modifying operating system (OS) and application settings.

Anti-malware - software that scans computers to protect from malicious software such as spyware, adware, and worms.

Authenticated Scan – an authenticated scan obtains accurate vulnerability information on assets by authenticating with the required level of system access to obtain detailed and accurate information about the operating system and installed software.

Authentication - the process by which users, processes, or services provide proof of their identity.

Availability – the principle that authorized users have timely and reliable access to information and IT resources.

Backup – a copy of computer files and data stored in an alternate location so it can be recovered if it is lost or becomes corrupted.

Baseline Configuration - documented, formally reviewed and agreed-upon specifications that ensure that IT Assets are properly configured and hardened to reduce vulnerabilities.

Blacklist – a list of common words or characters disallowed for user passwords due to their potential for exploit.

Business Continuity Plan (BCP) - documentation of a predetermined set of instructions or procedures that describe how an organization's mission/business processes will be sustained during and after a significant disruption.

Business Impact Analysis (BIA) – identifies critical business functions and documents the potential impacts resulting from disruption.

Bring Your Own Device (BYOD) – refers to the use of personally used devices for access to university IT resources.

Certificate – digital information that provides verification and authentication for a website. Certificates, also known as SSL (Secure Socket Layer) certificates, are used to ensure internet security by preventing third parties with malicious intent from intercepting, reading, or modifying any information transmitted.

Change Management - a critical discipline that controls and communicates the changes occurring in the IT environment.

CIO - Chief Information Officer - the CIO directs Information Technology Services for the University.

CISO - Chief Information Security Officer - the FSU CISO directs the Information Security and Privacy Office (ISPO) for the University.

Compensating Control - a temporary solution mechanism that is put in place to manage security risk and meet a security objective that is otherwise deemed impractical to implement at the present time. Compensating controls should only be considered when a specific security requirement or security control objective cannot be met due to legitimate technical or documented business or legal constraints. Compensating controls are required

to sufficiently manage or mitigate the risk associated with the vulnerability by implementing other alternative controls.

Compromised Credentials - the unauthorized disclosure of a password, token, or other user credentials can provide access to organizational systems or data. The credential may become compromised through various means, such as phishing, malware, social engineering, or accidental means.

Consolidated University Unit (CUU) – a consolidated group of related university units that has management authority and responsibility for compliance with IT policies, standards and guidelines.

Consolidated University Unit (CUU) Dean, Director, Department Head (DDDH) - the Dean,

Director, Department Head or other managerial position responsible for protecting the confidentiality, availability, and integrity of university information assets within a CUU. The CUU DDDH has responsibility for ensuring IT security and privacy for the units within the CUU.

Consolidated University Unit (CUU) Information Security Manager (ISM) - the liaison designated by the CUU Dean, Director or Department Head (DDDH) responsible for coordinating the CUU's information security program. The CUU ISM is the central point of contact between the University Units and ISPO for security issues.

Consolidated University Unit (CUU) Privacy Coordinator - the liaison designated by the CUU Dean, Director or Department Head (DDDH) responsible for coordinating the CUU's privacy program. The CUU Privacy Coordinator is the central point of contact between the University Units and ISPO for privacy issues.

Continuity of Operations Plan (COOP) – a COOP focuses on restoring an organization's mission-essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations. Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP. NIST 800-34, Rev 1 Contingency Planning Guide for Federal Information Systems

Confidential Data - data protected by federal and state laws or rules, FSU contractual obligations or privacy considerations. Disclosure could cause harm to individuals and/or the University, including criminal and civil liability.

Confidentiality – the principle that information is accessible only to those authorized (authorized access).

Cookies - short text files stored on a user's device by a website. Cookies are normally used to provide a more personalized experience and to remember user profiles without the need of a specific login.

Critical Business Functions - critical operational and/or business support functions that cannot be interrupted or unavailable for more than a mandated or predetermined timeframe without significantly jeopardizing University operations.

Cryptography – the discipline that embodies the principles and methods for the transformation of data to hide semantic content, prevent unauthorized use, or prevent undetected modification. Cryptography is a method to protect data and includes both encryption (which is reversible) and hashing (which is not reversible, or "one way").

Cybersecurity Readiness Scorecard – a report provided by ISPO to FSU executive leadership on overall cybersecurity posture of CUUs and associated units. Metrics include compliance with information security and privacy policies, and utilization of security products provided by the University and the CUU/Unit technology environment.

Data at Rest – data residing in files systems, distributed desktops and large, centralized data stores, databases, or other storage methods.

Data in Transit - data that is actively moving from one location to another, such as across the internet, through a private network, or between devices and systems.

Data Controller - the University or individual University Unit personnel who determines the purposes and means of processing personal data subject to the GDPR regulation.

Data Custodian – the Dean, Director, Department Head (DDDH) or other manager who is ultimately responsible for the integrity, accurate reporting and use of university data resources.

Data Manager – the university unit employee(s) delegated operational oversight responsibility for data resources by the Data Custodian.

Data Subject - A natural person about whom FSU holds personal data and who can be identified, directly or indirectly, by reference to that personal data.

Data User - FSU faculty members, staff members, trainees, volunteers, agents, contractors, students, and any person FSU has provided an FSU ID.

Disaster Recovery Plan – a written plan that defines technical activities that enable the continued availability or recovery of IT systems and services to an acceptable level of performance. A DR plan is used to address significant disruptions to service that deny access to primary facility infrastructure for an extended period.

Disruption - an unplanned event that causes an information system to be inoperable (e.g., minor or extended power outage, extended unavailable network, or equipment or facility damage or destruction).

EAR - Regulations set forth in parts 730-774, inclusive, of Title 15 of the Code of Federal

Regulations. EAR Regulates dual-use items not covered by ITAR, but still applies to some defense related items.

Education record - records that contain information directly related to a student and which are maintained by an educational agency or institution or by a party acting for the agency or institution. See 34 CFR Section 99.3 for a complete definition of "education records" and a list of records that are not included in the definition.

Encryption – the process of changing plaintext data into ciphertext through the use of a cryptographic algorithm for the purpose of security or privacy.

FERPA - the Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99) is a federal law that protects the privacy of student education records. Florida Statute 1002.22 requires FSU to protect the disclosure and access to student education records in accordance with FERPA.

FIPA - the Florida Information Protection Act (FIPA) protects the security of confidential personal information.

FISMA – the Federal Information Security Management Act is a federal law passed in 2002 that requires federal agencies to develop, document, and implement an information security and privacy program.

FSU Data – data created or received by data users while acting on behalf of FSU. Does not include intellectual property, which by law, copyright or other policies is owned, licensed or otherwise legally controlled by a data user.

GDPR - the General Data Protection Regulation is the regulation in European Union (EU) law on data protection and privacy in the EU and the European Economic Area (EEA). It also addresses the transfer of personal data outside the EU and EEA.

GLBA – the Gramm-Leach-Bliley Act requires financial institutions to safeguard sensitive data and explain their information sharing practices to their customers.

Hardening - the process of securing an IT Asset's configuration and settings to eliminate as many security risks as possible to reduce vulnerability and the possibility of being compromised. Hardening reduces an asset's "surface of vulnerability", which is larger when a system performs more functions; a single-function system is more secure than a multipurpose one. Reducing available ways of attack may include changing default passwords, removing unnecessary software, removing unnecessary usernames or logins, and disabling or removing unnecessary services.

High Risk Data - data that is collected, developed, maintained, or managed by or on behalf of FSU and is protected by law, contracts, university patents, or to mitigate institutional risks. Any information that could, if exposed, create civil or criminal penalties, reputational damage, or loss of protected intellectual property.

HIPAA - the Health Insurance Portability and Accountability Act of 1996 is a federal law that provides data privacy and security provisions for safeguarding patient medical information.

Incident Response (IR) Plan - documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of malicious cyberattacks against an organization's information system(s).

Industry Standard - a document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context. Note: Standards should be based on the consolidated results of science, technology, and experience, and aimed at the promotion of optimum community benefits.

Information Assets – institutional (business) data, personal data, applications, information systems, computers, network devices and paper documents that are created, accessed, managed and/or controlled by the university.

Information Security Incident - a suspected, attempted, successful, or imminent threat of unauthorized access, use, disclosure, breach, modification, or destruction of information; interference with information technology operations; or significant violation of responsible use policy.

Infrastructure - all of the resources of a network that make network or internet connectivity, management, business operations and communication possible. Network infrastructure allows for effective communication and service between users, applications, services, devices and so forth.

Institutional Data - any data that is owned, licensed by, or under the direct control of the university, whether stored locally or with a cloud provider.

Integrity – the principle that assures information remains intact, correct, authentic, accurate and complete. Integrity involves preventing unauthorized and improper creation, modification, or destruction of information.

Interference - the degradation of a wireless communication signal caused by electromagnetic radiation from another source. Such interference can either slow down a wireless transmission or eliminate it depending on the strength of the signal.

Internet of Things (IoT) - devices that are connected to the internet. IoT devices include sensors, controllers, and household appliances.

ITAR (International Traffic In Arms) - the United States regulation that controls the manufacture, sale, and distribution of defense and space-related articles and services as defined in the United States Munitions List (USML).

ISPO - Information Security and Privacy Office. This office is led by the Chief Information Security Officer (CISO).

IT Assets - technology resources including, but not limited to, computers, networks, servers, applications, databases, software, and operating systems owned by, managed by or sponsored by IT Asset Custodians.

ITGC – the Information Technology Governance Council, made up of FSU Vice Presidents.

Low Risk Data - data not classified as High or Moderate Risk that is designated as publicly available, without requiring the specific information custodian's approval. Low Risk data

does not expose FSU to financial loss or jeopardize the security of information assets or physical security.

Malware - a program inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim. A compromise can be in the form of a virus, worm, Trojan, or a backdoor (which can give an attacker access to a compromised system around any security mechanisms).

Media Sanitization - the erasure, overwriting, or destruction of storage media to the extent that data cannot be recovered using standard system functions or software data recovery utilities.

Misconfiguration - an incorrect or suboptimal configuration of an information system or system component that may lead to vulnerabilities.

Mission Critical - any factor (component, equipment, personnel, process, procedure, software, etc.) that is essential to business operations. Mission Critical IT systems and data enable essential IT functions that would have an immediate detrimental effect on the University and CUUs if there was an interruption or failure of services including, but not limited to, one or more of the following:

- Risk to human life or safety
- Significant impact on the University's research, learning and teaching, and administrative functions
- Significant legal, regulatory or financial costs
- Loss of access to critical data or the ability to carry out critical business functions following an event

Mitigation - a temporary solution to minimize a threat's negative impact when it cannot be eliminated.

Moderate Risk Data - information that is not explicitly protected by legal or contractual mandates but for which unauthorized access or a modification could cause financial loss, damage to FSU's reputation, violate an individual's privacy rights or make legal action necessary.

MOU – Memorandum of Understanding.

Multi-Factor Authentication (MFA) – a security enhancement that requires at least two pieces of evidence (your credentials) when logging in to an account. Credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Credentials must come from at least two different categories to enhance security.

National Institute of Standards and Technology (NIST) – agency responsible for developing standards and guidelines, including minimum requirements, used by federal agencies in providing adequate information security for the protection of agency operations and assets.

Office of Foreign Access Control (OFAC) - The Office of Foreign Assets Control administers and enforces economic sanctions programs primarily against countries and groups of individuals, such as terrorists and narcotics traffickers. The sanctions can be either comprehensive or selective, using the blocking of assets and trade restrictions to accomplish foreign policy and national security goals.

Patch - a "repair job" for a piece of programming; also known as a "fix". A patch is the immediate solution to an identified problem that is provided to users; it can sometimes be downloaded from the software maker's Web site.

PCI DSS - the Payment Card Industry Data Security Standard defines compliance requirements for any company that accepts, stores, processes, or transmits credit card information that protects the privacy and security of consumers.

Personal identifiable information (PII) - any information relating to an individual or identifiable natural person. An identifiable person can be identified, directly or indirectly – in particular, by reference to an identification number or to one or more factors specific to physical, physiological, mental, economic, cultural or social identity.

Personal Information - any information used to identify data subjects.

Personally Owned Device – any non-FSU owned smartphone, tablet, laptop, notebook or other IT device used to access technology resources.

Phishing - an attempt to trick someone into clicking on a link to install ransomware or other programs that can lock you out of your data and spread laterally on the network to other systems or to reveal information (e.g., a password) that can be used to attack systems or networks.

Privacy - the condition achieved when successfully maintaining the confidentiality of personal, student or employee information transmitted over a network.

Privacy by Design - a framework based on proactively embedding privacy into the design and operation of IT systems, networked infrastructure, and business practices.

Privileged Access - an elevated or higher level of access to university IT (Information Technology) systems or data resources than would be granted to a standard user account and ordinary user**.** Privileged access requires explicit authorization to perform functions considered to be of a sensitive or confidential nature when accessing university systems, tools, or data.

Privileged Account - a university user account with the approved authorizations of a privileged user.

Privileged User – a user that is trusted and authorized to perform elevated security functions or operations, which include access to confidential data that non-privileged user accounts and ordinary system users are not authorized to perform.

Process Account - a non-interactive account used to provide access to resources or services within an application or across applications.

Red Flags Rule - created by the Federal Trade Commission, along with other government agencies such as the National Credit Union Administration, to help prevent identity theft.

Reliability – the principle that IT resources consistently perform according to specifications.

Remediation – removing cybersecurity threat(s) by patching or fixing weaknesses detected in assets, networks, and applications.

Reputational Harm - often called reputation risk, is the potential loss of financial capital, social capital and/or market share resulting from damages to a firm's reputation.

Restricted Data - data for which the unauthorized disclosure may have moderate adverse effects on the University's reputation, resources, services, or individuals.

Residual Risk – the portion of risk remaining after security measures have been applied.

Retention - the minimum time necessary to retain records before they have met their administrative, legal, fiscal, or historical usefulness, as set forth by the Florida Department of State, other regulations, and contractual requirements.

Risk - a measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of the adverse impacts that would arise if the circumstance or event occurs and the likelihood of occurrence.

Risk Acceptance – the decision to accept responsibility for an identified security risk.

Risk Mitigation - prioritizing, evaluating, and implementing the appropriate risk-reducing controls/countermeasures recommended from the risk management process.

Risk Remediation – eliminating cybersecurity threat(s) by removing or fixing weaknesses detected in assets, networks, and applications.

Risk Tolerance - the organization's readiness to bear the risk after risk treatment in order to achieve its objectives.

Risk Transfer – shifting of a security risk from one party to another.

Risk Assessment - the process of identifying, estimating, and prioritizing information security risks

Security - Security, as used in this policy, not only includes measures to protect electronic communication resources from unauthorized access but also includes the preservation of resource availability and integrity.

Security Configuration Management - the management and control of configurations for an information system with the goal of enabling security and managing risk. The process includes identifying, controlling, accounting for, and auditing changes made to pre-established Baseline Configurations.

Sensitive Personal Information - Special categories of Data (e.g., racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union memberships, genetic data, biometric data, data concerning health and data concerning a natural person's sex life or sexual orientation) for which applicable law provides enhanced protections.

Service Account - an interactive account provided by the software vendor to be used only for access required at the highest level within the application.

Service Level Agreement (SLA) - A service contract that represents a commitment between a service provider and one or more customers and addresses specific aspects of the service, such as responsibilities, details on the type of service, expected performance level (e.g., reliability, acceptable quality, and response times), and requirements for reporting, resolution, and termination.

Significant Harm - the permanent loss of revenue to the organization.

Social Security Act - 42 U.S.C. § 401 et seq. | (1935) established a permanent national old-age pension system through employer and employee contributions; later it was extended to include dependents, the disabled, and other groups.

Software Development Life Cycle (SDLC) - A formal or informal methodology for designing, creating, and maintaining software (including code built into hardware).

Solution - The key design, architectural, and implementation choices made by organizations to satisfy specified security requirements for systems or system components.

Spam - unwanted and unsolicited email or material created or knowingly disseminated in such a large volume that it tends to disrupt the proper functioning of university information technology resources or individuals' ability to use such resources. Spam is most often sent to a large number of email accounts and may be used to deliver malware or links to malicious websites.

Tabletop Exercise - a discussion-based simulation of an emergency in an informal, stress-free environment; designed to elicit constructive scenario-based discussions.

Third-Party Vendor/Provider - a company or entity with whom FSU has a written agreement or is seeking an agreement to provide a product or service.

Threat – any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information or denial of service.

University Unit - a school or college and any departments or divisions which are a subdivision of a college or school; centers, facilities, labs, libraries, or programs within a

college or school, or as an independent entity; offices; associations; and administrative units.

University Unit Dean, Director, Department Head (**DDDH) -** the Dean, Director, Department Head or other managerial position responsible for protecting the confidentiality, availability, and integrity of university information assets within a University Unit. The DDDH has management authority and responsibility for IT security and privacy for the unit, in coordination with their designated CUU's information security program.

University Unit Information Security Manager (ISM) – the liaison designated by a University Unit Dean, Director or Department Head (DDDH) responsible for ensuring a University Unit's compliance with security IT policies, standards and guidelines, in coordination with their designated CUU's information security program.

University Unit Privacy Coordinator - the liaison designated by a University Unit Dean, Director or Department Head (DDDH) responsible for ensuring a University Unit's compliance with privacy IT policies, standards and guidelines, in coordination with their designated CUU's information privacy program.

Vulnerability - a weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Vulnerability Scanner - Vulnerability scanners are automated tools that allow organizations to check if their networks, systems, and applications have security weaknesses that could expose them to attacks.

Wireless Infrastructure - Refers to wireless access points, antennas, cabling, power, and Network hardware associated with the deployment of a wireless communications network.