TEXAS A&M INTERNATIONAL UNIVERSITY™

29.01.99.L1.00 Definitions

Approval date: 03/28/13
Revision date: 01/24/13
Next scheduled review date: as needed
Author: Office of Information Technology

Abuse of Privilege: When a user willfully performs an action prohibited by organizational policy or law, even if technical controls are insufficient to prevent the user from performing the action.

Academic Affairs: Team member will advise team regarding the processes within Academic Affairs.

Accessibility: Web design criteria, which supports access that is not dependent on a single sense or ability, such as vision or hearing.

Active Directory (AD): An account management system which makes it possible for users to obtain and access electronic resources at TAMIU, using a single username and password.

Application Custodian: The guardian or caretaker of the application; the person(s) charged with implementing the controls specified by the owner of the application. This custodian is responsible for any errors or application updates. Application custodians are responsible for testing the functionality of the application after any major change performed by either the application custodian or system custodian.

Backup: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.

Banner: TAMIU's Student Information System.

Banner Security Officer: Person responsible for monitoring and implementing security controls and procedures for Banner.

Change: Any implementation of new functionality, any interruption of service, any repair of existing functionality, and/or any removal of existing functionality.

Change Management: The process of controlling modifications to hardware, software, firmware, and documentation to ensure that Information Resources are protected against improper modification before, during, and after system implementation.

CIA triad: Confidentiality, Integrity and Availability.

Cloud Storage: Data is maintained, backed up and managed online and available over the network (Internet).

Compliance Officer: Person responsible for monitoring, facilitating, and ensuring University compliance with all federal and state laws, Texas A&M University System (TAMUS) policies and regulations, state agency directives and requirements, Southern Association of Colleges and Schools (SACS), Equal Employment Opportunity (EEO), and Affirmative Action (AA).

Computer Incident Response Team (CIRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

Confidential Information: Information that must be protected from unauthorized disclosure or public release based on state or federal law (e.g. the Texas Public Information Act and other constitutional, statutory, judicial, and legal agreements).

Examples of "Confidential" data may include, but are not limited to the following:

- Personally Identifiable Information, such as: a name in combination with Social Security number (SSN), Date of Birth (DOB) and/or financial account numbers
- Banner ID in combination with Social Security number (SSN), Date of Birth (DOB) and/or financial account numbers
- Student Education Records
- Intellectual Property, such as: certain intellectual property as set forth in section 51.914 of the Texas Education Code
- Medical Records (as defined by HIPAA)

Custodian: Guardian or caretaker; the holder of data; the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. For server applications, Information Services is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

Empowered Official: Individual who is responsible for overseeing export/import control regulations at TAMIU.

Data Center: The facility used to house servers and network systems.

Data Owner: A person or department having responsibility and authority for the data.

Device Wipe: Restores device to factory default settings and erases all data from the device.

DMZ: (Demilitarized Zone) an area, a physical or logical subnetwork, where external facing services reside and are accessible to an untrusted network such as the Internet. Also known as a perimeter network.

DREAD: A classification scheme for quantifying, comparing and prioritizing the amount of risk presented by each evaluated threat. The DREAD acronym stands for: **D**amage Potential, **R**eproducibility, **E**xploitability, **A**ffected Users and **D**iscoverability.

Electronic mail (email): Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.

Electronic mail system: Any computer software application that allows electronic mail to be communicated from one computing system to another.

Emergency Change: When an unauthorized, immediate response to imminent critical system failure is needed to prevent widespread service disruption.

Exchange ActiveSync: Protocol that communicates over the web, designed for the synchronization of email, calendar, tasks, and notes from the University's email server to a mobile device.

External storage media: Portable devices that are not permanently fixed inside a computer; they are used to store data. These include, but are not limited to, USB thumb drives, CDs, DVDs, external hard drives, memory cards, cloud storage, etc.

FERPA: Family Educational Rights and Privacy Act.

File Owner: The holder (assignee) of the computer account which controls a file. Not necessarily the owner in the sense of property.

HIPAA: The Health Insurance Portability and Accountability Act of 1996.

Incident Report: Form that must be completed when an emergency change occurs.

Incident Response Team (IRT): Personnel responsible for coordinating the response to computer security incidents in an organization.

Intrusion detection system (IDS): a system or software that monitors activities of networks or systems for malicious activities or policy violations capable of producing reports of such information.

Information Resources (IR): Any computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing websites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, tablets, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), smartphones, telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it includes the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information Resources Manager (IRM): Person responsible to the State of Texas for management of the agency's information resources. The designation of an agency information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the agency's information activities, and ensure greater visibility of such activities within and between State agencies. The IRM has been given the authority and the accountability by the State of Texas to implement security policies, procedures, practice standards and guidelines to protect the Information Resources of the agency. At TAMIU, the IRM is the Associate Vice President for IT/CIO.

Information Resource Owner: an entity responsible for:

1. a business function, and
2. determining controls and access to information resources supporting that business function.

IRT Team: In an effort to help mitigate IT security related incidents, TAMIU formed the IT Incident Response Team (IRT). The IRT will hold regular meetings to review any incidents that have occurred, and will discuss projects relating to IT Security. Emergency meetings may also

be called at the discretion of the CIO or ISO if an incident needs immediate attention. The team members and their roles include: ISO, FERPA Officer, PCI Compliance Representative, Financial Services, Academic Affairs, Risk Management & Compliance, Judicial Affairs, UPD Representative.

Information Security Administrator (ISA): Person responsible for monitoring and implementing security controls and procedures for a system.

Information Security Officer (**ISO**)**:** Person responsible to the executive management for administering the information security functions within the University. The ISO is TAMIU's internal and external point of contact for all information security matters.

Information Security Officer: Team member will advise team of incidents that have occurred and will update members on security projects.

Information Services (IS): The name of the agency department responsible for computers, networking and data management. This definition is interchangeable with (OIT).

Internet: A global system interconnecting computers and computer networks. The computers and networks are owned separately by a host of organizations, government agencies, companies, and colleges. The Internet is the present "information super highway."

Intranet: A private network for communications and sharing of information similar to the Internet, but accessible only to authorized users within an organization. An organization's intranet is usually protected from external access by a firewall.

ISAAC – Information Security Assessment Awareness and Compliance: This system provides an information security risk assessment methodology and reporting function for individual departments and TAMIU.

Judicial Affairs: Team member will advise team of student judicial affairs.

FERPA Officer - Team member will advise team of all aspects regarding FERPA, as well as enrollment management processes.

Financial Services – Team member will advise the team of all financial operations for students.

Key Public Entry Point (KPEP): A Web page that a state agency or institution of higher education has specifically designed for members of the general public to access official information (e.g., the governing or authoritative documents) from the agency or institution of higher education.

Local Area Network (LAN): A data communications network spanning a limited geographical area, a few miles at most. It provides communication between computers and peripherals at relatively high data rates and relatively low error rates.

Malicious Code: Software which interferes with the normal operation of information resources. It includes, but is not limited to, viruses, worms, Trojan horses, backdoors, and attack scripts.

Metadata: Data about data; index-type data used to identify, describe, locate, or preserve (other) data over time.

NetID: Single sign on credential for most University systems.

Network Scanning: The procedure used for identifying active hosts on a network. This also extends to finding network addresses that do no map to a specific host.

Office of Information Technology (OIT): The name of the TAMIU department responsible for computers, networking and data management.

Offsite Storage: A geographically different location from the University campus that does not share the same disaster threats. Based on an assessment of the data backed up and its criticality, removing the backup media from the building and storing it in another secured location on the University campus may be appropriate.

Owner: The manager or agent responsible for the function which is supported by the resource, the individual upon whom responsibility rests for carrying out the program that uses the resources. The owner is responsible for establishing the controls that provide the security. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments.

Password: A string of characters which serves as authentication of a person's identity, which may be used to grant, or deny, access to private or shared data.

PCI Compliance Representative: Team member will advise team regarding PCI Compliance, as well as Business and Finance processes.

Peer-to-Peer (P2P): An approach to content distribution in which digital files are transferred between "peer" computers over the internet. As a new channel for content distribution, P2P changes the conventional hierarchy of information. The roles of producer, consumer, and gatekeeper of digital content blur, and more information and resources can be delivered to more people and applications than otherwise would be possible.

Personal computing device: Any device that is not property of Texas A&M International University and can receive or transmit data to and from IR. See portable computing devices definition for more information.

POP: Post Office Protocol. Email storage protocol.

Portable Computing Devices: Any easily portable device that is capable of receiving and/or transmitting data to and from IR. These include, but are not limited to, notebook computers, handheld computers, tablets and cell phones.

Production System: The hardware, software, physical, procedural, and organizational issues that need to be considered when addressing the security of an application, group of applications, organizations, or group of organizations.

Recovery: retrieving data from hard drives, solid-state drives, storage tapes, and other media internal or external that is corrupted, inaccessible or damaged physically or logically.

RIAA: Recording Industry Association of America works to protect the intellectual property and First Amendment rights of artists and music labels; conduct consumer, industry and technical research; and monitor and review state and federal laws, regulations and policies.

Risk Management & Compliance: Team member will advise team of risk and compliance matters.

Rootkits: A set of software tools used by a third party after gaining access to a computer system in order to conceal the altering of files, or processes being executed by the third party without the user's knowledge.

Scheduled Change: Formal notification received, reviewed, and approved by the review process in advance of the change being made.

Security Administrator: The person charged with monitoring and implementing security controls and procedures for a system. Whereas each agency will have one Information Security Officer, technical management may designate a number of security administrators.

Security Incident: Assessed event of attempted entry, unauthorized entry, or an information attack on an automated information system. It includes unauthorized probing and browsing, disruption or denial of service, altered or destroyed input, processing, storage, or output of information, or changes to information system hardware, firmware, or software characteristics with or without the users' knowledge, instruction, or intent.

Server: A computer dedicated to running one or more such services, to serve the needs of programs running on other computers on the same network.

Server Hardening: the enhancement of server security through different means, which result in a more secure server operating environment due the measures established during this process.

Service Set Identifier (SSID): The assigned name for a wireless network.

Software: A computer program which provides instructions to computer hardware. System software such as Windows or Mac OS, operate the machine itself. Application software such as spreadsheet or word processing programs provides specific functionality.

Standard Operating Procedure (SOP): Set of detailed instructions for performing a specific process.

STRIDE: A classification scheme for characterizing known threats according to the kinds of exploits that are used (or motivation of the attacker). The STRIDE acronym stands for: **S**poofing identity, **T**ampering with data, **R**epudiation, **I**nformation disclosure, **D**enial of service, and **E**levation of privilege.

Strong Passwords: A strong password is a password that is not easily guessed. It is normally constructed of a sequence of characters, numbers, and special characters, depending on the capabilities of the operating system. Typically, the longer the password, the stronger it is. It should never be a name, dictionary word in any language, an acronym, a proper name, a number, or be linked to any personal information about the user such as a birth date, social security number, and so on.

System Administrator: Person responsible for the effective operation and maintenance of Information Resources, including implementation of standard procedures and controls to enforce an organization’s security policy.

System Custodian: Guardian or caretaker of the operating system and physical hardware; the person(s) charged with implementing the controls specified by the owner of the system. This custodian is responsible for operating system updates and assisting the Application Custodian with any testing or major changes to the system.

System Development Life Cycle (SDLC): A set of procedures to guide the development of production application software and data items. A typical SDLC includes design, development, maintenance, quality assurance and acceptance testing.

Third Party: An external entity that supplies goods or services including but not limited to vendors and other Universities members of the Texas A&M system.

TRAIL: The Texas Records and Information Locator and Electronic Depository Program (TRAIL/EDP) is an automated system used to collect, index, and preserve electronic state publications. To ensure that publications are appropriately harvested and indexed, a publishing entity must include metadata in its online publications.

Trojan Horse: Destructive programs—usually viruses or worms—that are hidden in an attractive or innocent-looking piece of software, such as a game or graphics program. Victims may receive a Trojan horse program by e-mail or on a diskette, often from another unknowing victim, or may be urged to download a file from a Web site or bulletin board.

University Campus Homepage: The main page for the University.

Unscheduled Change: Failure to present notification to the formal process in advance of the change being made. Unscheduled changes will only be acceptable in the event of a system failure or the discovery of a security vulnerability.

UPD Representative: Team member will advise team of any criminal computer incidents.

Usability: Web design criteria that support user performance, ease of navigation, and understandability.

User: An individual, automated application or process that is authorized to access the resource by the owner, in accordance with the owner's procedures and rules.

Vendor: Someone who exchanges goods or services for money.

Virtual Private Network (VPN): A network which utilizes public telecommunications infrastructure to conduct private data communications via an encrypted connection.

Virus: A program that attaches itself to an executable file or vulnerable application and delivers a payload that ranges from annoying to extremely destructive. A file virus executes when an infected file is accessed. A macro virus infects the executable code embedded in Microsoft Office programs that allow users to generate macros.

Vulnerability: a weakness or flaw in system security design, implementation, procedures or controls that can cause a violation of the system's security policy or a security breach if exploited by an attacker.

W3C: World Wide Web Consortium

Wardriving: The act of searching for Wireless networks throughout a given area.

WebFocus: Web-based report system which is used to create custom reports for Banner.

Web page: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).

Web server: A computer that delivers (*serves up*) web pages.

Web site: A location on the World Wide Web accessed by typing its address (URL) into a Web browser. A Web site always includes a home page and may contain additional documents or pages.

World Wide Web: A system of Internet hosts that supports documents formatted in HTML (HyperText Markup Language) which contains links to other documents (hyperlinks) and to audio, video, and graphic images. Users can access the Web with special applications called browsers, such as Mozilla Firefox, Navigator, and Microsoft Internet Explorer.

Worm: A program that makes copies of itself elsewhere in a computing system. These copies may be created on the same computer or may be sent over networks to other computers. The first use of the term described a program that copied itself benignly around a network using otherwise unused resources on networked machines to perform distributed computation. Some worms are security threats, using networks to spread themselves against the wishes of the system owners, and disrupting networks by overloading them. A worm is similar to a virus in that it makes copies of itself, but different in that it need not attach to particular files or sectors at all.