29.01.99.Z1.07 Guideline: Definitions

Approved February 13, 2013

Supplements HSC Information Resources Guidelines

Reason for the Guidelines

This appendix defines words or phrases used within Texas A&M University System Health Science Center (HSC) information resource rules and SAP’s. This document will be updated as needed.

1. Definitions

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.

Accessible: Designed to support access by all users in a variety of ways and not dependent on a single sense or ability.

Accessibility: Allows people with disabilities to perceive, understand, navigate, and interact with EIR.

Asymmetric Encryption (or Public Key Cryptography (PKC) or Public Key Encryption): A method of encryption in which two different keys are used: one for encrypting and one for decrypting the data (a public and a private key). Only one key (the private key) must be kept secret. The key that is exchanged (the public key) poses no risk if it becomes known.

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

Change:

- any implementation of new functionality
- any interruption of service
- any repair of existing functionality
- 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.
**Computer Incident Response Team (CIRT):** Personnel responsible for coordinating the response to computer security incidents in an organization.

**Confidential Information:** Information that is excluded from disclosure requirements under the provisions of applicable state or federal law, e.g., the Texas Public Information Act. Examples of “Confidential” data may include, but are not limited to: Personally identifiable information such as a name in combination with social security number (SSN) and/or financial account numbers, student education records, intellectual property such as copyrights, patents, trade secrets, and medical records.

**Crypto Ignition Key (CIK):** A device or electronic key used to unlock the secure mode of crypto-equipment.

**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 mainframe applications, OIT is the custodian; for micro and mini applications, the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.

**Demilitarized Zone (DMZ):** A physical or logical sub-network that contains and exposes an organization's external services to a larger untrusted network.

**Electronic and Information Resources (EIR):** Includes information technology and any equipment or interconnected system or subsystem of equipment that is used in the creation, conversion, duplication, storage, or delivery of data or information. The term includes, but is not limited to, telecommunications products (such as telephones), information kiosks and transaction machines, websites, multimedia, and office equipment such as copiers and fax machines. The term does not include any equipment that contains embedded information technology that is used as an integral part of the product, but the principal function of which is not the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

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

**Electronic Mail (Email) System:** Any computer software application that allows electronic mail to be communicated from one computing system to another.

**Encryption (encrypt, encipher, or encode):** The conversion of plaintext information into a code or ciphertext using a variable, called a “key” and processing those items through a fixed algorithm to create the encrypted text that conceals the data’s original meaning.

**Exception:** A justified, documented non-conformance with one or more standards or specifications of Chapter 206 and/or Chapter 213 of the Texas Administrative Code, which has been approved by the Office of the President or designee.

**External Facing Server:** Any server that has services that are accessible outside of the HSC network without the use of a VPN.
**Firewall:** An access control mechanism that acts as a barrier between two or more segments of a computer network or overall client/server architecture, used to protect internal networks or network segments from unauthorized users or processes.

**Full disk encryption (FDE) (or Whole Disk Encryption):** A kind of disk encryption software or hardware which encrypts every bit of data that goes on a disk or disk volume. The term "full disk encryption" is often used to signify that everything on a disk, including the programs that can encrypt bootable operating system partitions, but they must still leave the Master Boot Record (MBR), and thus part of the disk, unencrypted.

**Host:** A computer system that provides computer service for a number of users.

**Information Attack:** An attempt to bypass the physical or information security measures and controls protecting an IR. The attack may alter, release, or deny data. Whether an attack will succeed depends on the vulnerability of the computer system and the effectiveness of existing countermeasures.

**Information Operations:** Actions taken to affect adversary information and information systems while defending one’s own information and information systems.

**Information Resources (IR):** Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, 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, personal digital assistant (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is 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 Management Act:** Texas Government Code chapter 2054. States that information and information resources possessed by agencies of state government are strategic assets belonging to the residents of this state that must be managed as valuable state resources;

**Information Resources Manager (IRM):** Responsible to the State of Texas for management of the agency/university’s information resources. The designation of an agency/university information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the state 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. If an agency does not designate an IRM, the title defaults to the agency’s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

**Information Security Officer (ISO):** Responsible to the executive management for administering the information security function within the agency. The ISO is the university’s internal and external point of contact for all information security matters.
Information Technology (IT) (as used in the EIR definition): Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.

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 that, like the Internet, is based on TCP/IP, but is accessible only to authorized users within an organization. An organization’s intranet is usually protected from external access by a firewall.

Key: A parameter that determines the functional output of a cryptographic algorithm. Without a key, the algorithm would have no result. In encryption, a key specifies the particular transformation of plaintext into ciphertext, or vice versa during decryption. Keys are also used in other cryptographic algorithms, such as digital signature schemes and message authentication codes.

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/Malware: Software designed to operate in a manner that is inconsistent with the intentions of the user, typically to modify, destroy, or steal information, use up resources, or allow unauthorized access to information systems. Examples of such software include: viruses, Trojan horses, worms, and spyware

Mission Critical Information: Information that is defined by the University or information resource owner to be essential to the continued performance of the mission of the University or department. Unavailability of such information would result in more than an inconvenience. An event causing the unavailability of mission critical information would result in consequences such as significant financial loss, institutional embarrassment, failure to comply with regulations or legal obligations, or closure of the University or department.

Mobile Hotspot: A device connects to the Internet via a cellular network, and then creates a Wi-Fi hotspot that can connect any Wi-Fi-enabled device within about 30 feet.

Network Vulnerability Scanning: The process of performing a vulnerability assessment to determine the presence of security vulnerabilities in an information system.

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

Offsite Storage: Based on data criticality, offsite storage should be in a geographically different location from the HSC campus that does not share the same disaster threat event. Based on an assessment of the data backed up, removing the backup media from the building and storing it in another secured location on the HSC 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.

**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, PDAs, pagers, 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.

**Proprietary Encryption:** An algorithm that has not been made public and/or has not withstood public scrutiny. The developer of the algorithm could be a vendor, an individual, or the government.

**Registration Authority (RA):** The person in the public key infrastructure (PKI) who verifies network user requests for a digital certificate and tells the certificate authority (CA) to issue it.

**Scheduled Change:** A notification is 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 institution will have one ISO, technical management may designate a number of security administrators.

**Security Incident:** In information operations, an 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.

**Sensitive Personal Information:** An individual’s first name or first initial and last name in combination with any one or more of the following items, if the name and the items are not encrypted Social security number Driver’s license number or government-issued identification number or Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

**Server:** A computer program that provides services to other computer programs in the same, or another, computer. A computer running a server program is frequently referred to as a server, though it may also be running other client (and server) programs.
**Service Set Identifier (SSID):** The name of a wireless local area network (LAN). All wireless devices on a wireless LAN must employ the same SSID in order to communicate with each other.

**Spyware:** A program that hides within a computing system with the purpose of collecting information and activities and reporting them back to the spyware distributor. Examples include credit card numbers, email addresses, web surfing habits, etc.

**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 you such as a birth date, social security number, and so on.

**Symmetric Encryption (Cryptosystem):** A method of encryption in which the same key is used for both encryption and decryption of the data. The sender uses the key and algorithm to encrypt, and the receiver uses both to decrypt. Both sender and receiver must possess the key, which must remain private.

**Symmetric Key:** An encryption methodology in which the encryptor and decryptor use the same key, which must be kept secret or private. Symmetric key algorithms in common use are designed to have security equal to their key length.

**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 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.

**Technical Accessibility Standards:** Standards for EIR that enable accessibility for all users as mandated in Title 1, Chapter 213, Subchapter C and Title 1, Rule §206.70, Subchapter C of the Texas Administrative Code.

**Texas Public Information Act:** Texas Government Code Chapter 552, gives you the right to access government records; and an officer for public information and the officer's agent may not ask why you want them. All government information is presumed to be available to the public. Certain exceptions may apply to the disclosure of the information.

**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.

**Unscheduled Change:** Little to no notification is given 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.
**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:** A person who supplies goods or a service to a governmental entity or another person directed by the entity. The term does not include a state agency or institution, except for Texas Correctional Industries. The term includes an officer or employee of a state agency or institution when acting in a private capacity to supply goods or a service.

**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.

**Vulnerability Assessment:** The process of transmitting data through a network to elicit responses in order to determine configuration state about an information system. This includes port scanning and the verification of security controls for the information resource.

**Web Application Firewall:** A form of firewall which controls input, output, and/or access from, to, or by an application or service.

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

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

**Website:** 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.

**Wireless Access:** A type of local area network (LAN) that uses high frequency radio waves rather than wires to communicate between nodes. A wireless LAN spans a relatively small area using one or more of the following technologies to access information resources systems:

**Wireless Handheld Devices:** Includes text-messaging devices, tablets, personal digital assistants (PDA’s) and smart phones.

**Wireless Local Area Network:** Based on the IEEE 802.11 family of standards.

**Wireless Personal Area Network:** Based on the Bluetooth and/or infrared (IR) technologies.

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

OFFICE OF RESPONSIBILITY:

Vice President for Finance and Administration