Procedure Definitions and References

Introduction

These are the special usage definitions and references used throughout the various information security policies and procedures. Where a word or phrase does not appear in this list, the common usage will apply.

Definitions

1. **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.
2. **Accellion:** Secure FTP server used to send or receive large files.
3. **Acceptable Use Policy (AUP):** Policy that a user must agree to follow in order to be provided with access to a network or to the Internet.
4. **Argos**: The institutionally supported platform for report development.
5. **Backup**: Copy of files and applications made to avoid loss of data and facilitate recovery in the event of a system crash.
6. **Banner**: TAMUK's Student Information System.
7. **Banner Internet Native Banner (INB):** This is the administrative interface into Banner.
8. **Category-I Data:** Sensitive data that must be protected from unauthorized disclosure or public release based on federal or state law or Texas A&M University - Kingsville rules and regulations (e.g., HIPAA, FERPA, HEOA, Sarbanes-Oxley, Gramm-Leach-Bliley, the Texas Identity Theft Enforcement and Protection Act, Texas A&M University System Policies). University data that are not otherwise protected by a known statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.) are included in this category.
   Examples of "Category-I" data may include but are not limited to:
   a. Personally Identifiable Information, such as: a name in combination with Social Security Number (SSN) and/or financial account numbers
   b. Student Education Records
   c. Intellectual Property, such as: Copyrights, Patents and Trade Secrets
   d. Medical Records
9. **Category-II Data:** University data not otherwise identified as Category-I data, but which are subject to disclosure or release in accordance with the Texas Public Information Act. Such data must be appropriately protected to ensure a controlled and lawful release.
   Examples of "Category-II" data may include but are not limited to:
   a. email
   b. personnel records
   c. information security procedures
   d. research
   e. internal communications
10. **Category-III Data:** University data not otherwise identified as Category-I or Category-II data but which are intended or required for public release as described in the Texas Public

Information Act. Such data have no requirement for confidentiality, integrity, or availability.

11. **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.
12. **Change**:
    a. any implementation of new functionality
    b. any interruption of service
    c. any repair of existing functionality
    d. any removal of existing functionality
13. **Computer Incident Response Team (CIRT)**: Personnel responsible for coordinating the response to computer security incidents in an organization
14. **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 iTech is the custodian; for micro and mini applications the owner or user may retain custodial responsibilities. The custodian is normally a provider of services.
15. **Emergency Change**: When an unauthorized immediate response to imminent critical system failure is needed to prevent widespread service disruption.
16. **Electronic mail system**: Any computer software application that allows electronic mail to be communicated from one computing system to another.
17. **Electronic mail (email)**: Any message, image, form, attachment, data, or other communication sent, received, or stored within an electronic mail system.
18. **E-mail**: Abbreviation for electronic mail.
19. **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.
20. **Host**: A computer system that provides computer service for a number of users.
21. **Incident Management:** The monitoring and detection of security events on a computer or computer network, and the execution of proper responses to those events.
22. **Individual-Specific Database**: An Institutional Data element qualifies as Individual-Specific Data if it is generated and maintained by an individual affiliated with the University as an employee, contractor, or student within the scope of that individual's relationship with the University and if it is not generally communicated to or used by other members of the University community.
23. **Information Attack**: An attempt to bypass the physical or information security measures and controls protecting an Information Resource. 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.
24. **Information Operations**: Actions taken to affect adversary information and information systems while defending one's own information and information systems.
25. **Information Resources (IR)**: The procedures, equipment, and software that are employed, designed, built, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information, and associated personnel including consultants and contractors. (Texas Government Code §2054.003)
26. **Information Resources Manager (IRM)**: 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 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.

27. **Information Security Officer (ISO)**: Responsible to the IRM for administering the information security functions within the agency. The ISO is the agency's internal and external point of contact for all information security matters.
28. **Institutional Data:** A data element qualifies as Institutional Data if it is:
    a. Generated or collected in the course of or in furtherance of the business of the University;
    b. Exists in digital form, capable of being electronically stored or transmitted; and
    c. Resides or resided at any time in the past on any University-owned computer, server, or storage medium.
    d. Paper records that do not meet these criteria are not subject to this policy, although they may be subject to other, similar policies of the University.
29. **Intrusion Detection:** Intrusion detection systems provide the first line of defense for identification of threats from external sources. Intrusion detection provides early warning of potential internet and network based threats.
30. **Information Technology (IT):** Information Resources
31. **iTech:** Information Technology -The department responsible for University information resources.
32. **iTech Banner Security Officer (BSO)**: Person responsible for monitoring and implementing security controls and procedures for Banner.
33. **IT Project**: A temporary endeavor undertaken to create a unique IT product, implement a service or produce a result.
34. **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."
35. **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.
36. **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.
37. **Offsite Storage**: Based on data criticality, offsite storage should be in a geographically different location from the Texas A&M University-Kingsville 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 Texas A&M University-Kingsville campus may be appropriate.
38. **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

39. **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.
40. **PMI**: Project Management Institute
41. **Portable Computing Devices**: Any easily portable device that is capable of receiving and/or transmitting data to and from Information Resources. These include, but are not limited to, notebook computers, handheld computers, PDAs, pagers, and cell phones.
42. **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.
43. **Project Management**: The application of knowledge, skills, tools and techniques to mitigate risk, control budget and manage scope of tasks.
44. **Remediation:** Action taken to resolve security weaknesses in computer systems.
45. **Risk**: A vulnerability, either potential or realized, that could be exploited to provide unauthorized or unintended behavior by an IT component resulting in potential reductions in the confidentiality, integrity or availability of information. Risks may originate from inadequate processes, hardware or software design, or any aspect associated with the provision and support of information resources.
46. **Risk Assessment:** To assess potential options for reducing or mitigating vulnerabilities identified during the risk analysis.
47. **Risk Management Cycle**: The process through which the risks associated with information resources are identified and then eliminated or managed. Risk management plans will be generated or updated annually.
48. **Scheduled Change**: Formal notification received, reviewed, and approved by the review process in advance of the change being made.
49. **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.
50. **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.
51. **Security Monitoring:** Automated tools that will provide real time notification of detected wrongdoing and vulnerability exploitation.
52. **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.
53. **Server Hardening:** Procedures to strengthen the security posture of a server to prevent unauthorized access.

54. **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.
55. **System Administrator**: Person responsible for the effective operation and maintenance of IR, including implementation of standard procedures and controls, to enforce an organization's security policy.
56. **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.
57. **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.
58. **University Data**: An Institutional Data element qualifies as University Data if it is:
    a. Neither Unit-Specific nor Individual-Specific Data as defined below; and is
    b. Relevant to planning, managing, operating, controlling, or auditing administrative functions of an administrative or academic unit of the University; or
    c. Generally referenced or required for use by more than one organizational unit; or
    d. Included in an official University administrative report; or
    e. Used to derive an element that meets one or more of the criteria above.
59. **Unit-Specific Data:** An Institutional Data element qualifies as Unit-Specific Data if it is:
    a. Uniquely pertinent to the work of a single office or unit and used and accessible solely by individuals within that office or unit. While correspondence and other documents (whether in print, electronic or digital formats) may contain University Data subject to this policy, correspondence and documents themselves will generally not qualify as University Data applying the above criteria. Ownership of and access to correspondence and documents created or received by University personnel are governed by the Texas A&M System on Records Management, the University Intellectual Property Policy, the Public Information Act.
60. **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.
61. **User**: An individual or automated application or process that is authorized access to the resource by the owner, in accordance with the owner's procedures and rules. Has the responsibility to (1) use the resource only for the purpose specified by the owner, (2) comply with controls established by the owner, and (3) prevent disclosure of confidential or sensitive information. The user is any person who has been authorized to read, enter, or update information by the owner of the information. The user is the single most effective control for providing adequate security.
62. **Vendor**: someone who exchanges goods or services for money.
63. **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.

64. **Vulnerability Scanning:** The automated process of proactively identifying security vulnerabilities of computing systems in a network in order to determine if and where a system can be exploited and/or threatened.
65. **Web page**: A document on the World Wide Web. Every Web page is identified by a unique URL (Uniform Resource Locator).
66. **Webserver**: A computer that delivers (serves up) web pages.
67. **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.
68. **Wireless:** Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor.
69. **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 Netscape, Navigator, and Microsoft Internet Explorer.
70. **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.

References

1. Copyright Act of 1976
2. Computer Fraud and Abuse Act of 1986
3. Computer Security Act of 1987
4. DIR Practices for Protecting Information Resources Assets
5. DIR Standards Review and Recommendations Publications
6. Foreign Corrupt Practices Act of 1977
7. The Health Insurance Portability and Accountability Act of 1996 (HIPAA)
8. IRM Act, 2054.075(b)
9. The State of Texas Information Act
10. The State of Texas Penal Code, Chapters 33 and 33A
11. Texas Administrative Code, Chapter 202
12. Texas A&M University-Kingsville Procedure 29.01.03.K1.010
13. Texas A&M University-Kingsville Procedure 29.01.04.K1.010
14. Texas Government Code, Section 441