

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

21.01.06.C2.01 Definitions

Approved June 11, 2007

Supplements University Rule 21.01.06.C2

1. GENERAL

Throughout Texas A&M University-Corpus Christ procedures related to University Rule 21.01.06.C2 Security of Electronic Information Resources, the following definitions shall apply. The Texas Administrative Code 202.1 Applicable Terms and Technologies for Information Security can also be used to provide additional guidance.

2. DEFINITIONS

- 2.1. Account – information resource users are typically assigned logon credentials that include, at the minimum, a unique user name, and password.
- 2.2. Anomalous activity – workstation, server, or network work activity that is unusual or out of the ordinary and may be the indicator of malware or malicious user activity.
- 2.3. Authentication mechanisms – account names and passwords, security access cards, tokens, and keys associated with mechanisms that permit access to facilities, information resources, or data.
- 2.4. Business continuity – the availability of critical resources and the continuity of operations to facilitate the effective operation of university business-related activities.
- 2.5. Change –
 - (1) any implementation of new functionality,
 - (2) any interruption of service,
 - (3) any repair of existing functionality, and
 - (4) any removal of existing functionality.
- 2.6. Confidential information – Information that is exempted from disclosure requirements under the provisions of the Texas Public Information Act or other applicable state or federal laws. Most student records are confidential records.
- 2.7. Contractor – any company, and its employees, not affiliated with Texas A&M University-Corpus Christi, which provides a service to the university.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 2.8. Custodian – A person (or department) providing operational support for an information system and having responsibility for implementing owner-defined controls and access privileges.
- 2.9 External media storage devices – any external device that is capable of storing electronic data. Examples of external media storage devices include but are not limited to: USB drives, flash media, floppy disks, CD/DVD-ROM, external hard drives, MP3 players, iPods, cellular phones, cameras, etc.
- 2.10. File owner – Holder (assignee) of the computer account which controls a file. Not necessarily the owner in the sense of property.
- 2.11. Intranet – the university’s network that is used to interconnect the university’s information resources and, when permitted, allow the connection of those resources to the Internet.
- 2.12. Internet – a worldwide, publicly accessible network of interconnected computer networks.
- 2.13 Incident Response Plan – an organized approach to addressing and managing situations involving information resources and Sensitive Information in a manner that limits damage and reduces recovery time and costs.
- 2.14. Information resources – The procedures, equipment, and software that are designed, employed, operated, and maintained to collect, record, process, store, retrieve, display, and transmit information or data.
- 2.15. Information resource facility – the physical locations (rooms, closets, crawlways, cable conduit, etc) that house the supporting infrastructure and physical information resources used to manage Sensitive Information.
- 2.16. ISAAC – Information Security Awareness, Assessment, and Compliance System. ISAAC allows departments to register and perform a baseline security risk assessment of their information systems and perform the following functions:
- (1) develop a Business Continuity/Disaster Recovery Plan for your information systems and data,
 - (2) perform an automated, web-based risk analysis,
 - (3) perform a physical security check of your premises,
 - (4) find links to Security Awareness Training resources, and
 - (5) ensure compliance with state and local information security standards.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 2.17. Malware – Software that is designed to operate in a manner that is inconsistent with the intentions of the user and which typically results in annoyance or damage to the user's information systems. Examples of such software include:
- (1) viruses: Pieces of code that attach to host programs and propagate when an infected program is executed.
 - (2) worms: Particular to networked computers to carry out pre-programmed attacks that jump across the network.
 - (3) Trojan Horses: Hide malicious code inside a host program that appears to do something useful.
 - (4) attack scripts: These may be written in common languages such as Java or ActiveX to exploit weaknesses in programs; usually intended to cross network platforms.
 - (5) Spyware: Software planted on systems to capture and reveal information to someone outside the system. It can do such things as capture keystrokes while typing passwords, read and track e-mail, record the sites visited, pass along credit card numbers, and so on. It can be planted by Trojan horses or viruses, installed as part of freeware or shareware programs that are downloaded and executed, installed by an employer to track computer usage, or even planted by advertising agencies to assist in feeding the user targeted ads.
- 2.18. Mission critical information – Information that is defined by Texas A&M University-Corpus Christi or any division thereof (department, etc.), to be essential to their function(s) and would cause severe detrimental impact if the data/system were lost and unable to be restored in a timely fashion.
- 2.19. Mission critical service – a service or information resource 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 service or information resource would result in more than an inconvenience. An event causing the unavailability of mission critical service would result in consequences such as significant financial loss, institutional embarrassment, and/or failure to comply with regulations or legal obligations, or closure of the university or department.
- 2.20. Network extending or re-transmitting devices, systems and software – include, but are not limited to, the following: modems, hubs, routers, switches, wireless access points, ad hoc wireless interfaces, telecommunication voice devices, firewalls,

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

virtual private network servers, virtual network connection software, and Internet Anonymizer servers.

- 2.21. Network scanning – the process of transmitting data through a network to elicit responses in order to determine configuration state about an information system.
- 2.22. Network vulnerability scanning – the conduct of network scanning of an information system to determine the presence of security vulnerabilities in the information system.
- 2.23. Nondisclosure Agreement – a legal contract between at least two parties which outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict from generalized use.
- 2.24. Owner – A person responsible for a university function and for determining controls and access to electronic information resources supporting that university function.
- 2.25. Password/passphrase – a secret word, phrase, or code used to serve as a security measure in authentication mechanisms to protect against unauthorized access to information resources and data.
- 2.26. Phishing – The use of e-mails that appear to originate from a trusted source to trick a user into entering valid credentials at a fake website. Typically the e-mail and the web site look like they are part of a bank or some other legitimate e-commerce site with which the user conducts regular business.
- 2.27. Portable computing devices – mobile devices that can connect by cable, telephone wire, wireless transmission, or via any Internet connection to the university information technology infrastructure and/or data systems, such as, but not limited to, laptop computers, cellular phones, and Personal Digital Assistants (PDA).
- 2.28. Providing Entity – the university department that is permitting vendor access to their information resources.
- 2.29. Restricted personal information – Includes an individual's social security number, or data protected under state or federal law (e.g., financial, medical or student data).
- 2.30. Resource consolidation – the centralization of university information resources to reduce operational costs, increase server utilization, reduce real estate and facilities costs, improve availability, exploit new hardware platforms, and build an agile infrastructure able to respond more quickly to the rapidly changing requirements related to information technology.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 2.31. Resource custodian – See Custodian
- 2.32. Security baseline – the configuration of a network, the hosts on the network, and the applications on the host as detected by network, host, and application enumeration and vulnerability scanning tools. Information for a security baseline should be collected while the networks, hosts, and applications are operating in a "known good" state. Security baselines are used to detect changes in configuration and deployment to assist with the implementation of policy and detection of malicious activity.
- 2.33. Security incident – any violation of Federal or State laws and regulations, Texas A&M System Policies, or Texas A&M University-Corpus Christi Rules or Procedures.
- 2.34. Security patch – a fix to a program that eliminates a vulnerability exploited by malicious hackers.
- 2.35. Security testing – a combination of systems configuration testing, network scanning, and network vulnerability scanning to determine the state of an information resource and the services it provides.
- 2.36. Sensitive Information – any information identifiable as “Confidential Information,” “Mission Critical Information,” or “Restricted Personal Information” as outlined by the Texas Administrative Code 202.1 and the Texas Code of Criminal Procedure Article 2.29.
- 2.37. Software – A computer program, which provides the instructions which enable the computer hardware to work. System software, such as Windows or MacOS, operate the machine itself, and applications software, such as spreadsheet or word processing programs, provide specific functionality.
- 2.38. SPAM – the abuse of electronic messaging systems to send unsolicited bulk messages.
- 2.39. System administrator – See Custodian
- 2.40. System Development Life Cycle (SDLC) – a process used to develop and implement information resources, including requirements, validation, training, and user ownership through investigation, analysis, design, implementation, and maintenance. An SDLC should result in a high quality system that meets or exceeds customer expectations, within time and cost estimates, works effectively and efficiently in the current and planned information technology infrastructure, and is cheap to maintain and cost-effective to enhance.

UNIVERSITY PROCEDURES
TEXAS A&M UNIVERSITY-CORPUS CHRISTI

- 2.41. Texas Administrative Code 202 – information security standards for information resources purchased by agencies and institutions of higher education in the State of Texas.
- 2.42. University Technology Council (UTC) – a group of management level university faculty and staff members responsible for providing direction and guidance to the university in matters concerning and pertaining to the universities information resources.
- 2.43. User – An individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules.
- 2.44. Vendor – any company, and its employees, not affiliated with Texas A&M University-Corpus Christi, which provides a service to the university.
- 2.45. Wireless technologies – include, but are not limited to, any device capable of IEEE 802.11x, Bluetooth, Infrared, and/or cellular communications.

Contact for Interpretation: Assistant Vice President for Technology

Office of Responsibility: Executive Vice President, Finance & Administration