TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.01, Definitions

PURPOSE:

REVIEW:

POLICY/PROCEDURE:

1. **Access Point** is a device that allows computers or workstations to access the wired network by using radio transmissions. An access point contains transmit and receive antennas instead of ports for access by multiple wireless clients. Similar to standard wired "hubs," access points are shared bandwidth devices.

2. **Authentication** is the process of securing the identity of an individual based on a user account name and password. Authentication ensures the individual is who he or she claims to be, but does not address the access rights of the individual.

3. **Authorization** is the process of assigning individuals the permission to read, write, or modify system objects or execute transactions based on their identity.

4. **Broadcast Messages** are messages that are simultaneously sent out to multiple recipients.

5. **Cable (also referred to as cable modem)** is a type of Internet connection provided by the local cable company, used to transfer data at high speeds when compared to a dial-up modem.

6. **Chain Letters** are letters or emails directing the recipient to send out multiple copies so that its circulation increases exponentially.

7. **Computer Incident Response Team (CIRT)** is comprised of personnel responsible for coordinating the response to computer security incidents in the organization. Regular members will include:

    - Chief Information Officer or designee
    - Associate Vice President, Technology Services
    - Computer Security Analysts

    Depending on the nature and severity of the incident, the CIO or designee may appoint additional members to the CIRT from one or more of the following areas:

        - Other I.T. staff members with expertise in various operating systems and platforms
        - Human Resources representative
        - Physical Plant representative
        - Texas Tech Police
        - Media or public relations liaison

8. **Computer Security Analyst (CSA)** is an individual designated by the Information Technology (I.T.) Director at each campus location. The CSA will be appointed for each TTUHSC El Paso

regional campus and will coordinate virus protection activities at each campus under the direction of the Information Technology Security (ITS) group. The regional CSA will work closely with the Institutional Information Security Officer to implement security procedures, maintain locally administered security products, respond to security incidents, and coordinate the installation of patches on servers and workstations to correct security vulnerabilities.

9. **Computer Virus** is a program or piece of computer code that is installed or executed onto any computing device without the knowledge of the owner and runs against the owner's wishes. Most computer viruses will disrupt or alter the normal operation of the infected computer. Some computer viruses are destructive, permanently damaging data files or programs on a computer.

10. **Computing device** is an all-inclusive term referring to, but not limited to, desktop computer, laptop computer, Personal Digital Assistant (PDA), network, terminal, and any other computing device owned by the Institution.

11. **Custodian of an Information Technology Resource** is a person responsible for implementing owner-defined controls and access to an I.T. resource. (TAC 202.1(5))

12. **Distance Learning** is conducting live class sessions by holding discussions and delivering course content to geographically separated students in a fully interactive manner through the use of videoconferencing procedures, systems, and infrastructure.

13. A **Distance Learning Classroom** is a TTUHSC El Paso classroom equipped with a multi-media teaching podium, instructor video monitor, sound reinforcement system, student microphones, video cameras, VGA/video projector, projection screen, and associated items, connected to the TTUHSC El Paso network infrastructure for the purpose of conducting distance learning class sessions.

14. **e-Commerce** is a special web application that allows users to make online payments or purchases with a credit card.

15. **Firewalls** are security systems which control and restrict both network connectivity and network services, usually from the Internet. Firewalls establish a perimeter where access controls are enforced. Connectivity reflects which systems can exchange information. A service, sometimes called an application, refers to the way information flows through a firewall. Examples of services include FTP (file transfer protocol) and HTTP (web services).

16. **Host** is a hardware device that is connected to the TTUHSC El Paso network, and capable of transmitting and receiving data using Transmission Control Protocol/Internet Protocol (TCP/IP), the suite of communications transmission formats used to connect hosts on the Internet. Examples of hosts are personal computers, servers, printers, scanners, and network equipment.

17. **Information Security Officer (ISO)** is the individual appointed by the president or their designee and is responsible for administering the Institutional information security program. Under the direction of the CIO, the Information Security Officer is TTUHSC's at El Paso primary internal and external point of contact for all Information Technology security matters.

18. **Information Security Program** consists of the elements, structure, objectives and resources that provide information resource security for the Institution (TAC 202.1.8)

19. **Information Technology (I.T.) resources** include any and all hardware, software, and data used to create, store, process, and communicate information electronically as well as services to keep these resources current and operational.

20. **Information Technology Security Council (ITSC)** consists of representatives from each of the schools, and operational divisions; the CIO; the Associate Vice President of Technology Services; the Assistant Vice President of Information Services; the Information Technology Security Team; and the regional Computer Security Analysts. Each representative is appointed by executive management. The ITSC is responsible for insuring the Institutional security program aligns with Institutional business objectives.

21. **Information Technology Security (ITS) group** is newly formed within the I.T. Division and is comprised of the Information Security Officer and two Computer Security Analysts. Under the direction of the CIO, the ITS group is responsible for overseeing Institutional network security and computer virus protection activities.

22. **Interference** is the degradation of a communication signal, whether wired or wireless in origin, caused by electromagnetic radiation from another source. Such interference can distort, slow down, or completely eliminate the transmission of a communication signal, depending on the strength of the interference.

23. A **key public entry point** is defined as a web page that is specifically designed for members of the general public to access official Institution information. TTUHSC El Paso has designated the following as key public entry points:

    - the main Institutional home page (http://www.ttuhsc.edu),

24. A **Multi-media Teaching Podium** is the presentation device installed in each TTUHSC El Paso distance learning classroom, and containing a PC, digital tablet, document camera, computer screen, slide-to-video converter, VCR, user microphone, user control panel, and related network interface equipment.

25. **Network** is a system that transmits any combination of voice, video, and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all supporting hardware in between such as bridges, routers, multipoint control units, video codecs, and switches. In wireless systems, antennas, transmitters, and towers are also part of the network.

26. **Non-broadcast** refers to single site (non-TechLink) use of TTUHSC El Paso videoconferencing resources.

27. A **Notice of Disclaimer of Liability** is a statement repudiating the accuracy of the information contained on a web site and/or web page. A link to the Notice of Disclaimer of Liability must be included in the footer section of all key public entry points.

28. **Origination Site** refers to the TTUHSC El Paso distance learning classroom that is the controlling location in a videoconferencing session (usually the location where the instructor or presenter is physically present).

29. **Owner of an Information Technology Resource** is a person responsible: for a business function; and for determining controls and access to information resources supporting that business function. (TAC 202.1.10)

30. A **Regional Site Coordinator (RSC)** is the administrator of all local area networks (LAN) at each campus. The RSC is the contact person for all connectivity issues between the regional campus LAN's and the TTUHSC El Paso wide area network (WAN).

31. **Security** is defined as all measures to protect electronic hardware and software communication resources from unauthorized access and to preserve resource availability and integrity.

32. **Security Incident** is an event which results in unauthorized access, loss, disclosure, modification, disruption, or destruction of information resources whether accidental or deliberate. (TAC 202.1.14)

33. **Security Risk Analysis** is the process of identifying and documenting vulnerabilities and applicable threats to information resources. (TAC 202.1.15)

34. **Security Risk Assessment** is the process of evaluating the results of the risk analysis by projecting potential losses, assigning levels of risk, and recommending appropriate measures to remediate the risk. (TAC 202.1.16)

35. **Security Risk Management** are decisions to accept exposures or to reduce vulnerabilities to information resources. (TAC 202.1.17)

36. **Server** is a computer program that provides services, applications, and resources to computer users 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.

37. **TechLink** is all videoconferencing equipment, systems, infrastructure, and network used in distance learning, telemedicine, and general purpose videoconferencing at TTUHSC El Paso.

38. **Telemedicine** is the delivery of healthcare services to patients at distant locations through the use of videoconferencing procedures, systems, and infrastructure.

39. A **Telemedicine Consultation Facility** is a room equipped with a video camera, video monitor, videocassette player, and microphone, connected to the TTUHSC El Paso network infrastructure for the purpose of conducting telemedicine consultations and related videoconferencing activities.

40. An **Unauthorized Access Warning Banner** is a message informing the potential users of access restrictions to the system and is an important passive tool in assuring the security of TTUHSC El Paso computing system resources and the information contained therein.

41. **User** is an individual or automated application authorized to access an information resource in accordance with the owner-defined controls and access rules. (TAC 202.1.20)

42. **Videoconferencing Infrastructure** is defined as all network support equipment such as audio amplifiers, audio mixers, audio/video routers, CSU/DSUs, encoders, MCUs, PCs, software, touch panels, video codecs, video distribution amplifiers, video monitors, video quad mixers, video switchers, and similar devices installed in TTUHSC El Paso network control centers; and operated, maintained, and supported by the TTUHSC El Paso Information Technology Division for the purpose of providing distance learning, telemedicine, and general purpose video teleconferencing services to TTUHSC El Paso.

43. A **Videoconferencing Resource Reservation** is the confirmed allocation of videoconferencing resources to support a specific TechLink or non-broadcast event, or series of related events (such as recurring class sessions in a specific course).

44. A **Videoconferencing Resource Reservation Request** is an application by a user to schedule (or reserve) videoconferencing resources at TTUHSC El Paso.

45. A **Videoconferencing System** is defined as all interactive audio-visual equipment such as multi-media teaching podiums, video cameras, student microphones, video monitors, VGA/video

projectors, and related items installed in TTUHSC El Paso distance learning classrooms, conference rooms, telemedicine consultation rooms, and similar facilities, and supported and maintained by the TTUHSC El Paso Information Technology Division.

46. **Virtual Private Network (VPN)** is one or more encrypted connections over a shared public network, typically over the Internet, which simulates the behavior of direct, local connections.

47. A **web page** is defined as any information that is displayed through web browsers. It is the basic building block of web sites and is identified by a unique Universal Resource Locator (URL).

48. A **web site** is several inter-related and cross-linked web pages designed to function as a collective unit.

49. **Wireless Infrastructure** includes wireless access points, antennas, cabling, power, and network hardware associated with the deployment of a wireless communications network. This is also referred to as Wireless Local Area Networking, or WLAN.