TEXAS TECH UNIVERSITY HEALTH SCIENCES CENTER EL PASO

Operating Policy and Procedure

HSCEP OP: 56.40.06 – **Definitions**

REVIEW: This policy will be reviewed and updated in April of every Odd Numbered Year (ONY) by the Information Security Officer (ISO) and the Chief Information Officer (CIO), or when necessary as dictated by governing entities.

All other IT Policies can be found at https://ttuhscep.edu/it/policies/

POLICY/PROCEDURE:

Access is the physical or logical capability to view, interact with, or otherwise make use of information resources. 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.

Authentication is a mechanism employed to properly identify system users, processes acting on behalf of users, or devices, to validate the identities of those users, processes, or devices. The process of securing the identity of an individual based on a user account name and password.

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

Availability is the security objective of ensuring timely and reliable access to and use of information.

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

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.

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

Computer Incident Response Team (CIRT) is comprised of personnel responsible for coordinating the response to computer security incidents in the organization.

Regular members include:

- Chief Information Officer
- Information Security Officer
- Enterprise 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

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.

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.

Control is a safeguard or protective action, device, policy, procedure, technique, or other measure prescribed to meet security requirements (i.e., confidentiality, integrity, and availability) that may be specified for a set of information resources.

Encryption (encrypt or encipher) – the conversion of plaintext information into a code or cipher text 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.2

Enterprise Security Analyst (ESA) is an individual designated by the Information Technology Security Officer. ESA's work alongside the TTUHSC El Paso 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.

e-Commerce is a special web application that allows users to make online payments or purchases with a credit card. Federal Educational Rights and Protection Act (FERPA) is a federal law that protects the privacy and confidentiality of student educational records.3 Firewalls are security systems which control and restrict both network connectivity and network services.

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).

Guideline is a recommended, non-mandatory control that helps support standards or serve as a reference when no applicable standard is in place.4

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.

Information Custodian is a person, department agency, or third-party service provider responsible for implementing the information owner-defined controls and access to an information resource.5

Information Owner is a person with statutory or operational authority for specified information or information resources.6

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 El Paso's primary internal and external point of contact for all Information Technology security matters.

Information Security Program consists of policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish an information resources security function within an institution of higher education or state agency.7

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.

Information Security (IS) group is comprised of the Information Security Officer, an Associate Director, and Enterprise Security Analysts. Under the direction of the CIO, the IS group is responsible for overseeing institutional information security activities.

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.

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

Multi-media Teaching Podium is the presentation device installed in each TTUHSC El Paso distance learning classroom containing a user control panel and related network interface capabilities.

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.

Non-broadcast refers to an ad-hoc use of TTUHSC El Paso videoconferencing resources not utilizing IT support.

Notice of Disclaimer of Liability is a statement repudiating the accuracy of the information contained on a website 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.

Origination Site refers to the TTUHSC El Paso location that is the controlling site in a videoconferencing session (usually the location where the presenter is physically present).

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 (WAN).

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

Security Incident is an event which results in the accidental or deliberate unauthorized access, loss, disclosure, modification, disruption, or destruction of information or information resources.8

Security Risk Assessment is the process of identifying, evaluating, and documenting the level of impact on an organization's mission, functions, image, reputation, assets, or individuals that may result from the operation of information systems. Risk Assessment incorporates threat and vulnerability analyses and considers mitigations provided by planned or in-place security controls.9

Security Risk Management is the process of aligning information resources risk exposure with the organization’s risk tolerance by either accepting transferring, or mitigating risk exposures.10

Server is a computing device that provides services, applications, and resources to users. A computer running a server program is frequently referred to as a server though it may also be running other client (and server) programs.

TechLink is all videoconferencing equipment, systems, infrastructure, and network used in distance learning, telemedicine, and general purpose videoconferencing at TTUHSC (Lubbock).

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

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.

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 TTHSC El Paso computing system resources and the information contained therein.

User is an individual, process, or automated application authorized to access an information resource in accordance with federal state law agency policy the information owners’ procedures and rules. (TAC 202.1.38)

Videoconferencing Infrastructure is defined as all network support equipment installed on the TTUHSC El Paso network; and operated, maintained and supported by the TTUHSC El Paso Information Technology Department for the purpose of providing distance learning, telemedicine, and general purpose video conferencing services to TTUHSC El Paso.

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

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.

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.

Vulnerability Assessment is a documented evaluation containing information described in 2054.077(b), Texas Government Code which includes the susceptibility of a particular system to a specific attack.11

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).

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

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

1. TAC 202.1.1
2. TAC 202.1.13
3. 20 U.S.C §1232; 34 CFR Part 99, U.S. Department of Education
4. TAC 202.1.14
5. TAC 202.1.17
6. TAC 202. 1.18
7. TAC 202.1.21
8. TAC 202.1.34
9. TAC 202.1.32
10. TAC 202.1.33
11. TAC 202.1.39