

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.2	Definitions	Responsibility:	Chief Information Security Officer

DEFINITIONS

Definitions

ACCESS CONTROL EXECUTIVE (ACE): Each department has a designated ACE, who is responsible for managing the departmental users who have been granted access to PeopleSoft applications, the Document Review System, Data Warehouse, PeopleSoft business systems, and/or other business system databases.

CARDHOLDER DATA: At a minimum, cardholder data contains the full credit card primary account number (PAN). Cardholder data may also appear in the form of the full PAN plus any of the following:

- Cardholder name
- Expiration date
- Service code (the three- or four-digit security code on the back of the credit card; AMEX is on the front)

CHIEF INFORMATION SECURITY OFFICER (CISO): Responsible to the Information Resources Manager (IRM)/Vice President and Chief Information Officer (VP/CIO) for administering the information security functions within the University, including UT Medicine. The CISO is the University's primary internal and external point of contact for information security matters.

DATA OWNER: In most cases the data owner is the head of the department or division (Dean, Chair or Director). In most research organizations, or departments with a research mission, the data owner is the Principal Investigator that is responsible for the research study.

DEMILITARIZED ZONE (DMZ): A networking term used to describe an isolated network segment that has open access to the public network (Internet) but very restricted access inside the firewall to the protected side of the computer network. The DMZ serves as a security buffer between the two sides.

FILE TRANSFER PROTOCOL (FTP): A server/client application for transferring files between network devices.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.2	Definitions	Responsibility:	Chief Information Security Officer

IMS SERVICE DESK: The consolidation of help desks for Information Management and Services, managed by IMCSS. This is the direct link for TSRs to report timely information about information resource issues, as well as a focal point for customers for the following services:

- Computer support (e-mail, malware, technical support)
- Telephone support (telephones, new service, calling cards, repair)
- Mobile device support (cell phones, wireless access)
- Networking support (new service, connectivity)
- Password reset
- Blackboard support

INFORMATION MANAGEMENT CLIENT SUPPORT SERVICES (IMCSS): The Department of Information Management Client Support Services (IMCSS) was created to optimize and manage the client service functions of Information Management and Services (IMS). These functions include but are not limited to all help desk functions, billing for communications and customer support services, end user training and support, enterprise level computer support services and software (including Microsoft), phones and other telecommunications devices, Technical Support Representative (TSR) program, account management, and the Health Science Center Computer Store. The main goal for IMCSS is to provide exemplary customer support to students, staff, and faculty. IMCSS will concentrate on creating a “one stop” customer service center for IMS by leveraging teamwork, technology, expert knowledge, professionalism, and the commitment to excellence.

INFORMATION RESOURCES MANAGER (IRM): Responsible to the State of Texas for management of the University’s information resources. 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 University. The IRM for the Health Science Center is the Vice President and Chief Information Officer.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.2	Definitions	Responsibility:	Chief Information Security Officer

INFORMATION SECURITY COUNCIL: Information Security policy development is supported by the Information Security Council (ISC), a sub-committee of the Computing Resources Committee (CRC). As a standing Health Science Center committee, the CRC serves as the vehicle to present security policies to the Executive Committee for institutional approval and commitment.

INFORMATION SECURITY FUNCTION (ISF): Led by the Chief Information Security Officer, the ISF is responsible for security and risk management programs to protect information resource assets at the Health Science Center.

INFORMATION SECURITY AND ASSURANCE (ISA): Includes the CISO and information security analysts who are responsible for the tactical and operational execution of the information security functions within the University, including UT Medicine.

INTERNET PROTOCOL (IP): The communication standard used by the local computer network and the Internet.

INTERNET SERVICE PROVIDER (ISP): The organization that provides user access to the Internet.

OWNER: A person who:

- Has title to the property, possession of the property, whether lawful or not, or a greater right to possession of the property than the actor;
- Has the right to restrict access to the property; or,
- Is the licensee of data or computer software.

SECURE SHELL (SSH): A server/client application for securely connecting at a terminal level, generally at a command line interface, between a client and a host. The Telnet application does a similar function, over an insecure transport.

SYSTEM ADMINISTRATOR: An employee of the Health Science Center whose responsibilities include system, site, or network administration. System Administrators perform functions including, but

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.2	Definitions	Responsibility:	Chief Information Security Officer

not limited to, installing hardware and software, managing a computer or network, ensuring appropriate security is in place, and keeping information resources effective and operational.

SYSTEMS AND NETWORK OPERATIONS (SNO): The Department of Systems and Network Operations (SNO) provides information technology infrastructure services that include local and wide area network connectivity, data center management, and telephony. SNO works closely with ISA in implementing and monitoring security policies and procedures.

SYSTEM USER: Any individual who uses University information resources.

TECHNICAL SUPPORT REPRESENTATIVE (TSR): The departmental representative assigned the responsibility of receiving computer technology and security-related information from Computing Resources and ISA, and distributing that information as appropriate within their department. All TSRs should have a working knowledge of basic computer concepts.

TECHNICAL SUPPORT REPRESENTATIVE (TSR)/ADVANCED: A TSR who has received significant training, more technical proficiency in the department's environment, and information technology support duties as a primary job responsibility. Advanced TSRs may, at the discretion of the Dean, Chair or Director, be designated to receive additional security and related information from IMCSS and distribute that information as appropriate within their department.

TECHNICAL SUPPORT REPRESENTATIVE (TSR)/SYSTEM ADMINISTRATOR: An advanced TSR who is also a System Administrator.

TELECOMMUNICATIONS CUSTOMER SERVICE SPECIALIST: Staff that provide networking, telephone, and pager customer services (help desk) within SNO.

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.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	September 2004
Section 5.8	Information Security	Revised:	May 2011
Policy 5.8.2	Definitions	Responsibility:	Chief Information Security Officer

VENDOR: Someone who exchanges goods or services for money.

VIRTUAL LOCAL AREA NETWORK (VLAN): Constructs multiple private, logical network segments on a single physical transport media by means of Ethernet frame identifier (IEEE 802.10 specification).

VIRTUAL PRIVATE NETWORK (VPN): The networking software and hardware necessary to provide a secure transport of information between computers.
