

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.5	Information Management Client Support Services	Revised:	May 2001
Policy 5.5.11	Computer Crimes Law	Responsibility:	Vice President and Chief Information Officer

COMPUTER CRIMES LAW

State Law

Under state law, [Section 33.01, Title 7, Chapter 33, Texas Penal Code](#), it is a crime to make unauthorized use of protected computer systems or data files on computers or to make intentionally harmful use of such computers or data files. The seriousness of such a crime ranges from a misdemeanor to a felony. The complete text of the computer crimes chapter of the *Penal Code* appears below.

Definitions

ACCESS: means to approach, instruct, communicate with, store data in, retrieve or intercept data from, alter data or computer software in, or otherwise make use of any resource of a computer, computer network, computer program, or computer system.

AGGREGATE AMOUNT: means the amount of:

1. Any direct or indirect loss incurred by a victim, including the value of money, property, or service stolen or rendered unrecoverable by the offense; or
2. Any expenditure required by the victim to verify that a computer, computer network, computer program, or computer system was not altered, acquired, damaged, deleted or disrupted by the offense.

COMMUNICATIONS COMMON CARRIER: means a person who owns or operates a telephone system in this state that includes equipment or facilities for the conveyance, transmission, or reception of communications and who receives compensation from persons who use that system.

COMPUTER: means an electronic, magnetic, optical, electrochemical, or other high-speed data processing device that performs logical, arithmetic, or memory functions by the manipulations of electronic or magnetic impulses and includes all input, output, processing, storage, or communication facilities that are connected or related to the device.

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.5	Information Management Client Support Services	Revised:	May 2001
Policy 5.5.11	Computer Crimes Law	Responsibility:	Vice President and Chief Information Officer

COMPUTER NETWORK: means the interconnection of two or more computers or computer systems by satellite, microwave, line, or other communication medium with the capability to transmit information among the computers.

COMPUTER PROGRAM: means an ordered set of data representing coded instructions or statements that when executed by a computer cause the computer to process data or perform specific functions.

COMPUTER SERVICES: means the product of the use of a computer, the information stored in the computer, or the personnel supporting the computer, including computer time, data processing, and storage functions.

COMPUTER SYSTEM: means any combination of a computer or computer network with the documentation, computer software, or physical facilities supporting the computer or computer network.

COMPUTER SOFTWARE: means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.

COMPUTER VIRUS: means an unwanted computer program or other set of instructions inserted into a computer's memory, operating system, or program that is specifically constructed with the ability to replicate itself or to affect the other programs or files in the computer by attaching a copy of the unwanted program or other set of instructions to one or more computer programs or files.

DATA: means a representation of information, knowledge, facts, concepts, or instructions that is being prepared or has been prepared in a formalized manner and is intended to be stored or processed, is being stored or processed, or has been stored or processed in a computer. Data may be embodied in any form, including but not limited to computer printouts, magnetic storage media, laser storage media, and punch-cards, or may be stored internally in the memory of the computer.

EFFECTIVE CONSENT: includes consent by a person legally authorized to act for the owner. Consent is not effective if:

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.5	Information Management Client Support Services	Revised:	May 2001
Policy 5.5.11	Computer Crimes Law	Responsibility:	Vice President and Chief Information Officer

-
1. Induced by deception, as defined by Section 31.01, or induced by coercion;
 2. Given by a person the actor knows is not legally authorized to act for the owner;
 3. Given by a person who by reason of youth, mental disease or defect, or intoxication is known by the actor to be unable to make reasonable property dispositions;
 4. Given solely to detect the commission of an offense; or,
 5. Used for a purpose other than that for which the consent was given.

ELECTRIC UTILITY: has the meaning assigned by Subsection (c), Section 3, *Public Utility Regulatory Act* (Article 1446c, *Vernon's Texas Civil Statutes*).

HARM: includes partial or total alteration, damage, or erasure of stored data, interruption of computer services, introduction of a computer virus, or any other loss, disadvantage, or injury that might reasonably be suffered as a result of the actor's conduct.

OWNER: means a person who:

1. 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;
2. Has the right to restrict access to the property; or,
3. Is the licensee of data or computer software.

PROPERTY: means:

1. Tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or,

HEALTH SCIENCE CENTER HANDBOOK OF OPERATING PROCEDURES

Chapter 5	Information Management & Services	Effective:	June 2000
Section 5.5	Information Management Client Support Services	Revised:	May 2001
Policy 5.5.11	Computer Crimes Law	Responsibility:	Vice President and Chief Information Officer

2. The use of a computer, computer system, computer network, computer software, or data.

Breach of Computer Security

- A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.
- An offense under this section is a Class B misdemeanor unless in committing the offense the actor knowingly obtains a benefit, defrauds or harms another, or alters, damages, or deletes property, in which event the offense is:
 1. A Class A misdemeanor if the aggregate amount involved is less than \$1,500,
 2. A state jail felony if:
 - a. The aggregate amount involved is \$1,500 or more but less than \$20,000; or,
 - b. The aggregate amount involved is less than \$1,500 and the defendant has been previously convicted two or more times of an offense under this chapter,
 3. A felony of the third degree if the aggregate amount involved is \$20,000 or more but less than \$100,000.
- A person who is subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Defenses

It is an affirmative defense to prosecution under Section 33.02 that the actor was an officer, employee, or agent of a communications common carrier or electric utility and committed the proscribed act or acts in the course of employment while engaged in an activity that is a necessary incident to the rendition of service or to the protection of the rights or property of the communications common carrier or electric utility.
