## COMPUTER CRIMES LAW

### Policy

Under state law, the *Texas Penal Code*, **Title 7, Chapter 33**, Computer Crimes, it is a crime to make unauthorized use of protected computer systems or data files on computers, or networks, or to make intentionally harmful use of such computers or data files, or networks. The seriousness of such a crime ranges from a misdemeanor to a felony. Portions of the computer crimes chapter of the *Texas Penal Code* applicable to the Health Science Center appear below. This policy will be used to prosecute offenders under the state law by University Police, and to protect the Health Science Center from possible liability if University systems are misused.

Unless otherwise stated, any reference to “Section” refers to the Texas Penal Code. All paragraph numbering is derived from the Code, as are all terms and definitions.

### Sec 33.01 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.

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.

CRITICAL INFRASTRUCTURE FACILITY: means:

1. a chemical manufacturing facility;

2. a refinery;
3. an electrical power generating facility, substation, switching station, electrical control center, or electrical transmission or distribution facility;

4. a water intake structure, water treatment facility, wastewater treatment plant, or pump station;

5. a natural gas transmission compressor station;

6. a liquid natural gas terminal or storage facility;

7. a telecommunications central switching office;

8. a port, railroad switching yard, trucking terminal, or other freight transportation facility;

9. a gas processing plant, including a plant used in the processing, treatment, or fractionation of natural gas;

10. a transmission facility used by a federally licensed radio or television station; or

11. a cable television or video service provider headend.

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:

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 Section 31.002, Utilities Code.

**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.

**IDENTIFYING INFORMATION**: has the meaning assigned by Section 32.51.

**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

2. the use of a computer, computer system, computer network, computer software or data.
Section 33.02

Breach of Computer Security

(a) A person commits an offense if the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner.

(b) An offense under Subsection (a) is a Class B misdemeanor, except that the offense is a state jail felony if:

1. the defendant has been previously convicted two or more times of an offense under this chapter; or

2. the computer, computer network, or computer system is owned by the government or a critical infrastructure facility.

(b-1) A person commits an offense if with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses:

1. a computer, computer network, or computer system without the effective consent of the owner; or

2. a computer, computer network, or computer system:

   (A) that is owned by:

      (i) the government; or

      (ii) a business or other commercial entity engaged in a business activity;

   (B) in violation of:

      (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or

      (ii) a contractual agreement to which the person has expressly agreed; and

   (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system to defraud or harm another or alter, damage, or delete property.
(b-2) An offense under Subsection (b-1) is:

(1) a Class C misdemeanor if the aggregate amount involved is less than $100;

(2) a Class B misdemeanor if the aggregate amount involved is $100 or more but less than $750;

(3) a Class A misdemeanor if the aggregate amount involved is $750 or more but less than $2,500;

(4) a state jail felony if the aggregate amount involved is $2,500 or more but less than $30,000;

(5) a felony of the third degree if the aggregate amount involved is $30,000 or more but less than $150,000;

(6) a felony of the second degree if:

(A) the aggregate amount involved is $150,000 or more but less than $300,000;

(B) the aggregate amount involved is any amount less than $300,000 and the computer, computer network, or computer system is owned by the government or a critical infrastructure facility; or

(C) the actor obtains the identifying information of another by accessing only one computer, computer network, or computer system; or

(7) a felony of the first degree if:

(A) the aggregate amount involved is $300,000 or more; or

(B) the actor obtains the identifying information of another by accessing more than one computer, computer network, or computer system.
(c) When benefits are obtained, a victim is defrauded or harmed, or property is altered, damaged, or deleted in violation of this section, whether or not in a single incident, the conduct may be considered as one offense and the value of the benefits obtained and of the losses incurred because of the fraud, harm, or alteration, damage, or deletion of property may be aggregated in determining the grade of the offense.

(d) 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.

(e) It is a defense to prosecution under this section that the person acted with the intent to facilitate a lawful seizure or search of, or lawful access to, a computer, computer network, or computer system for a legitimate law enforcement purpose.

(f) It is a defense to prosecution under Subsection (b-1)(2) that the actor’s conduct consisted solely of action taken pursuant to a contract that was entered into with the owner of the computer, computer network, or computer system for the purpose of assessing the security of the computer, network, or system or providing other security-related services.

## Section 33.021
Online Solicitation of a Minor

(a) In this section:

(1) "Minor" means:

(A) an individual who is younger than 17 years of age; or

(B) an individual whom the actor believes to be younger than 17 years of age.

(3) "Sexual contact," "sexual intercourse," and "deviate sexual intercourse" have the meanings assigned by Section 21.01.

(4) "Sexually explicit" means any communication, language, or material, including a photographic or video image, that relates to or describes sexual conduct, as defined by Section 43.25.
(b) A person who is 17 years of age or older commits an offense if, with the intent to commit an offense listed in Article 62.001 (5)(A), (B), or (K), Code of Criminal Procedure, the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, intentionally:

(1) communicates in a sexually explicit manner with a minor; or

(2) distributes sexually explicit material to a minor.

(c) A person commits an offense if the person, over the Internet, by electronic mail or text message or other electronic message service or system, or through a commercial online service, knowingly solicits a minor to meet another person, including the actor, with the intent that the minor will engage in sexual contact, sexual intercourse, or deviate sexual intercourse with the actor or another person.

(d) It is not a defense to prosecution under Subsection (c) that the meeting did not occur:

(e) It is a defense to prosecution under this section that at the time conduct described by Subsection (c) was committed:

(1) the actor was married to the minor; or

(2) the actor was not more than three years older than the minor and the minor consented to the conduct.

(f) An offense under Subsection (b) is a felony of the third degree, except that the offense is a felony of the second degree if the minor is younger than 14 years of age or is an individual whom the actor believes to be younger than 14 years of age at the time of the commission of the offense. An offense under Subsection (c) is a felony of the second degree.

(g) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.
Section 33.03 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.

Section 33.04 Assistance By Attorney General

The attorney general, if requested to do so by a prosecuting attorney, may assist the prosecuting attorney in the investigation or prosecution of an offense under this chapter or of any other offense involving the use of a computer.

Section 33.05 Tampering With Direct Recording Electronic Voting Machine

(a) In this section:

(1) "Direct recording electronic voting machine" has the meaning assigned by Section 121.003, Election Code.

(2) "Measure" has the meaning assigned by Section 1.005 Election Code.

(b) A person commits an offense if the person knowingly accesses a computer, computer network, computer program, computer software, or computer system that is a part of a voting system that uses direct recording electronic voting machines and by means of that access:

(1) prevents a person from lawfully casting a vote;

(2) changes a lawfully cast vote;

(3) prevents a lawfully cast vote from being counted; or

(4) causes a vote that was not lawfully cast to be counted.

(c) An offense under this section does not require that the votes as affected by the person's actions described by Subsection (b) actually be the votes used in the official determination of the outcome of the election.
(d) An offense under this section is a felony of the first degree.

(e) Notwithstanding Section 15.01(d), an offense under Section 15.01(a) is a felony of the third degree if the offense the actor intends to commit is an offense under this section.

(f) With the consent of the appropriate local county or district attorney, the attorney general has concurrent jurisdiction with that consenting local prosecutor to investigate or prosecute an offense under this section.

Section 33.07
Online Impersonation

(a) A person commits an offense if the person, without obtaining the other person’s consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:

(1) create a web page on a commercial social networking site or other Internet website; or

(2) post or send one or more messages on or through a commercial social networking site or other Internet website, other than on or through an electronic mail program or message board program.

(b) A person commits an offense if the person sends an electronic mail, instant message, text message, or similar communication that references a name, domain address, phone number, or other item of identifying information belonging to any person:

(1) without obtaining the other person’s consent;

(2) with the intent to cause a recipient of the communication to reasonably believe that the other person authorized or transmitted the communication; and

(3) with the intent to harm or defraud any person.

(c) An offense under Subsection (a) is a felony of the third degree. An offense under Subsection (b) is a Class A misdemeanor, except that the offense is a felony of the third degree if the actor commits the offense with the intent to solicit a response by emergency personnel.
(d) If conduct that constitutes an offense under this section also constitutes an offense under any other law, the actor may be prosecuted under this section, the other law, or both.

(e) It is a defense to prosecution under this section that the actor is any of the following entities or that the actor's conduct consisted solely of action taken as an employee of any of the following entities:

1. a commercial social networking site;
2. an Internet service provider;
3. an interactive computer service, as defined by 47 U.S.C. Section 230;
4. a telecommunications provider, as defined by Section 51.002, Utilities Code; or
5. a video service provider or cable service provider, as defined by Section 66.002, Utilities Code.

(f) In this section:

1. "Commercial social networking site" means any business, organization, or other similar entity operating a website that permits persons to become registered users for the purpose of establishing personal relationships with other users through direct or real-time communication with other users or the creation of web pages or profiles available to the public or to other users. The term does not include an electronic mail program or a message board program.
2. "Identifying information" has the meaning assigned by Section 32.51.