

Policies for Information Systems Usage **(Revised 4/28/2004)**

The information systems (including computers, computer accounts, printers, network access, servers, host systems, software, electronic mail, Web pages, video systems, voice over IP and document imaging systems) at the University of Mary Hardin-Baylor (UMHB) are provided for the use of UMHB students, faculty and staff, as approved, in support of the programs of the university. All students, faculty and staff are responsible for seeing that these information systems are used in an effective, efficient, ethical and lawful manner. The use of information systems is a privilege, not a right, which may be revoked at any time for misuse. Users may not, under any circumstances, transfer or confer these privileges to other individuals. The following policies relate to their use.

1. The information systems are owned by the university and are to be used for university related activities only. All access to central information systems, including the issuing of accounts, must be coordinated through the Information Technology Department based upon approval of authorized personnel.
2. Information systems are to be used only for the purpose for which they are assigned and are not to be used for commercial purposes or non-university related activities. Use of university information system resources should compliment the university's mission and purpose. Registration of domain names using UMHB IP addresses is prohibited.
3. Computer programs, electronic mail, and electronic files are presumed to be confidential unless they have explicitly been made available to other authorized individuals. Authorized personnel (Information Technology Department) may access others' files when necessary for the maintenance and security of information systems. When performing maintenance, every effort will be made to provide the user with advance notice and to insure the safety and security of users' files as well as the information systems as a whole. Violations of policies regarding use of university information systems will be reported to the appropriate personnel.
4. Fraudulent, harassing, sexually explicit, pornographic, offensive or obscene messages or materials are not to be requested, sent, exchanged, printed, displayed, downloaded or stored. UMHB information systems resources should not be used in a manner "that would embarrass or bring discredit to the Baptist General Convention of Texas or to UMHB in the view of their constituencies." Chain letters, other forms of mass mailings, and non-UMHB official business related mailings are not allowed.
5. Others must not use a computer, computer account, Web page, or electronic mail account assigned to an individual. The individual is responsible for the proper use of the resource, including proper password protection. UMHB students, faculty, and staff must log out of unattended computers. All passwords must remain confidential and must not be revealed to anyone.

6. Information system accounts that expire or are terminated, along with the files in the accounts, will be deleted. Restrictions on storage space for e-mail files and messages will necessarily be imposed upon e-mail accounts due to physical hardware limitations.
7. Copyrighted material is not to be copied from or into except as permitted by law and/or by the contract or license agreement with the owner of the copyright. The use of copyrighted material on the UMHB local area network or on UMHB equipment must be in accordance with copyright license agreements.
8. No one should tamper with or deliberately attempt to degrade the performance of UMHB information systems and network services. Any malfunctioning or defective computer equipment and any servers performing unauthorized network administrative operations (i.e.: DHCP, DNS, POP3, SMTP, FTP Host, HTTP Host, etc.) will be disconnected without prior notification.
9. UMHB information systems and network services may not be extended to provide access to anyone outside of the UMHB community for any purpose without prior authorization from UMHB's Information Technology Department. Network services, including wires, network jacks, and wireless network access, may not be modified, extended or expanded beyond the original access point. Wireless network devices (i.e. routers, switches, hubs, access points, etc.) are not permitted to be connected to the UMHB network.
10. UMHB Information Technology Department reserves the right to restrict or deny access to any service that may be detrimental to its performance or utilize excessive bandwidth, such as audio or video downloads and on-line gaming.
11. Loopholes in the security of information systems must not be used to damage information systems, obtain extra resources, remove resources from another user, or gain access to or use unauthorized resources or files. Knowledge of such loopholes must be reported to the Information Technology Department immediately.

An individual's information systems usage privileges may be suspended immediately upon the discovery of a possible violation of these policies. Such suspected violations will be confidentially reported to the appropriate personnel.

Violations of these policies will be dealt with in the same manner as violations of other university policies and may result in disciplinary review. In such a review, the full range of disciplinary sanctions is available, including the loss of information systems usage privileges, dismissal from the university and legal action. Violations of some of the above policies may constitute a criminal offense under the Texas Penal Code (see V.T.C.A., Penal Code section 33.01 et seq.).

Computer Crimes Law

In 1985, a computer crimes law for the state of Texas took effect. This law was last amended in 2001. Under this state law, 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 Class B misdemeanor to third-degree felony.

Texas Computer Crimes Statute

Section 1. Title 7, Chapter 33, Texas Penal Code

Section 33.01. DEFINITIONS.

In this chapter:

- (1) “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.
- (2) “Aggregate amount” means the amount of:
 - (A) 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
 - (B) 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.
- (3) “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.
- (4) “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.
- (5) “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.
- (6) “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.

- (7) “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.
- (8) “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.
- (9) “Computer software” means a set of computer programs, procedures, and associated documentation related to the operation of a computer, computer system, or computer network.
- (10) “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.
- (11) “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 punchcards, or may be stored internally in the memory of the computer.
- (12) “Effective consent” includes consent by a person legally authorized to act for the owner. Consent is not effective if:
- (A) induced by deception, as defined by Section 31.01, or induced by coercion;
 - (B) given by a person the actor knows is not legally authorized to act for the owner;
 - (C) 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;
 - (D) given solely to detect the commission of an offense; or
 - (E) used for a purpose other than that for which the consent was given.
- (13) “Electric utility” has the meaning assigned by Section 31.002, Utilities Code.
- (14) “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.

(15) "Owner" means a person who:

(A) 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;

(B) has the right to restrict access to the property; or

(C) is the licensee of data or computer software.

(16) "Property" means:

(A) tangible or intangible personal property including a computer, computer system, computer network, computer software, or data; or

(B) the use of a computer, computer system, computer network, computer software, or data.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 1, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

Amended by Acts 1997, 75th Leg., ch. 306, § 1, eff. Sept. 1, 1997; Acts 1999, 76th Leg., ch. 62, § 18.44, eff. Sept. 1, 1999.

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 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;

(4) a felony of the second degree if the aggregate amount involved is \$100,000 or more but less than \$200,000; or

(5) a felony of the first degree if the aggregate amount involved is \$200,000 or more.

(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 his subject to prosecution under this section and any other section of this code may be prosecuted under either or both sections.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Amended by Acts 1989, 71st Leg., ch. 306, § 2, eff. Sept. 1, 1989; Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

Amended by Acts 1997, 75th Leg., ch. 306, § 2, eff. Sept. 1, 1997; Acts 2001, 77th Leg., ch. 1411, § 1, eff. Sept. 1, 2001.

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.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Renumbered from § 33.04 and amended by Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.

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.

Added by Acts 1985, 69th Leg., ch. 600, § 1, eff. Sept. 1, 1985. Renumbered from § 33.05 by Acts 1993, 73rd Leg., ch. 900, § 1.01, eff. Sept. 1, 1994.”