

UNIVERSITY *of* HOUSTON
MANUAL OF ADMINISTRATIVE POLICIES AND PROCEDURES

SECTION: Information Technology
AREA: Glossary

Number: 10.00.00

| |
|--|
| SUBJECT: Glossary of Information Technology Terms |
|--|

I. PURPOSE

This glossary defines terms that apply to University of Houston Information Technology MAPP policies and procedures.

II. DEFINITIONS

- A. Computer account: A unique access code used to provide secure access to a computer system. The code may be comprised of alphabetic and/or numeric characters and identifies an individual user to a computer system. A computer account often, but not always, requires some form of positive authentication (such as a protected password) before access is allowed. The computer account is required to manage access to the computer's resources. It is also used to identify the user in resource management and accounting systems.
- B. Computer application: A task to be performed by a computer program, series or programs, or system, such as payroll, student financial aid, or inventory tracking or management.
- C. Computer custodian: As used in these MAPPs, the person responsible for the physical security and use of the computer and the software installation.
- D. Computer Emergency Response Team: A group operating out of Carnegie Mellon University to investigate computer emergencies and security violations world-wide. The University of Houston has plans for an institutional CERT; i.e., an internal committee to investigate emergencies and violations of this type.
- E. Computer program: A formal expression of the sequence of actions required for a data processing task; the programmer's specification of the task(s) to the computer in a formal notation that can be processed by the computer. Consists of a series of statements and instructions that cause a computer to perform a particular operation or task.
- F. Computer-related equipment: Equipment used in the process of facilitating computing; generally includes computers, printers, modems, servers, and network connections and equipment.

- G. Computer system: A system that includes computer hardware, software, and people used to process data into useful information.
- H. Computer user: Any person--faculty, staff, student--who uses any university computer resources for any purpose.
- I. Computing devices: Any device used in the process of computing or communicating with other computers over any medium.
- J. Computing equipment: Equipment used to perform electronic calculations or other business activities such as word processing, desktop publishing, e-mail, etc.; usually refers to personal computers, monitors, keyboards, mainframe computers, minicomputers, and their associated peripheral devices.
- K. Computing and telecommunications resources: Any computer or telecommunications hardware, device, connector, modem cable, or software used by these devices to perform computing or telecommunications activities or functions.
- L. E-mail (electronic mail): Messages created, transmitted, and read completely on computers without necessarily being printed on paper.
- M. Ethernet: A local area network standard that uses radio frequency signals carried by coaxial cables, twisted pair wiring, or fiber to transmit data.
- N. Facility: For the purpose of information technology policies, guidelines, and procedures, a distinct physical location monitored and maintained by the University of Houston for the purpose of housing a cluster of computing, networking, or data processing equipment. A facility may be designated to provide specific services to specific university colleges or departments or may be open to all university users.
- O. Facility supervisor: The person charged with monitoring the general operations and administering policies and procedures at a university facility.
- P. Information security: The protection from tampering, destruction, or unauthorized access of records, data, or other information that is considered vital or sensitive to an organization, an individual, or a department within the organization.
- Q. Information security officer: The person charged with implementing and overseeing the tasks associated with information security of an organization.
- R. Initial screen banner: A greeting or message presented to users when they first access or attempt to access a computer system.

- S. Internet: A worldwide computer network available via telecommunications cables that connects universities, government laboratories and offices, businesses, and individuals around the world; commonly referred to as "the Information Superhighway."
- T. Mainframe computers: Computers with capabilities of large storage and computing capacity; normally capable of creating multiple virtual computers and having a variety of input/output options.
- U. Mini-computers: Computers that perform many of the functions of a mainframe on a reduced scale.
- V. Networking equipment: Any equipment used to transmit voices or information, such as bridges, routers, modems, servers, cabling, or software used by this equipment.
- W. Physically secured area: A room, hallway, building, or other defined area to which physical access is routinely denied to the general population or public. (Physical security may be accomplished by use of locked doors or gates, walls, and fences, and/or guards or monitors.)
- X. Security: See "information security."
- Y. Security violations: Damage, theft, or corruption of hardware, software, data, or other computing or telecommunications resources by individuals or events internal or external to the university.
- Z. Sniffer: A program designed to capture information going over the computer network intended for other programs or computer systems; may be used for benign or malicious purposes.
- AA. System accounting: Computer programs and data files that collect and report the use of computer system resources; includes use of permanent disk storage, processor time, and terminal connect time.
- BB. System administrator: The person responsible for the maintenance of software, programs, operating systems, and data files of a certain computing system; responsible for bug fixes, security holes, and back-ups. The system administrator may also manage the use of computing equipment, maintenance of computer accounts, and the resolution of user problems, issues, and needs.
- CC. University computing network: A combination of computing devices (bridges, routers, modems, etc.) and transmission media (fiber optic cable, coaxial cable, circuits, video, etc.) used by the University of Houston for both internal and external authorized computing and telecommunications activities.

- DD. University information security officer: Individual at the University of Houston who is responsible for information security.
- EE. Virus: A computer program that searches out other programs and infects them by embedding its own code. When the infected programs are run later, the embedded code executes and attempts to infect other programs. Viruses may do nothing other than propagate themselves. They may also produce any number of results that are not intended by the individual running the infected program.
- FF. World Wide Web, the Web, WWW: A global data network whose traffic consists of documents written in a specific language called "HyperText Mark-up Language," which supports text, pictures, audio, and video. Applications are available to view documents on the WWW that have an easy to use point-and-click interface that transfers the user to a screen with additional information on the subject.

III. REVIEW AND RESPONSIBILITY

Responsible Party: Associate Vice President, Information Technology

Review: Every 3 years, on or before September 1

IV. APPROVAL

C.R. Shomper

Associate Vice President, Information Technology

Date of Approval: July 15, 1996

V. REFERENCES

All Section 10 - Information Technology MAPPs

Index Terms: Computer terminology
Information technology terminology