

Memo to: All UH-Downtown/PS Holders
From: Max Castillo, President
Subject: Information Systems Security and Access Policy

UH - Downtown/PS 08.A.04
Issue No. 1
Effective date: 3/23/94
Page 1 of 1

1. PURPOSE

The purpose of this PS is to establish the legal use of Information Systems resources.

2. POLICY/PROCEDURES

2.1 Access to and use of computing resources is restricted to appropriately identified, authenticated, and authorized users. State law requires that state-owned information resources be used only for official state purposes.

2.2 The University of Houston - Downtown (UHD) is not exempt from the copyright laws concerning computer software. Unauthorized use or duplication of software is a federal crime. Title 17, Section 106 of the US code states *"It is illegal to make or distribute copies of copyrighted material without authorization"*. The only exception to this rule is the user's right to make a backup copy for archival purposes if the manufacturer does not provide one. Information Systems will maintain a list of federal and state laws which govern legal use of hardware and software.

2.3 All identification, passwords, telephone numbers, and other "access means" to information resources are proprietary to the state. Holders of such access means are accountable for unauthorized or negligent disclosure or use of access means including sharing of passwords (Vernon's Texas Code Annotated, Title 18 Penal Code 33.01 - 33.05).

2.4 All computer programs, software and electronic information that are part of university information systems are property of UHD and must not be copied or disclosed unless explicitly authorized in writing by appropriate management. This includes software developed for or by UHD and UHD-purchased software and its related documentation.

2.5 No software, program, or information can be added to, or removed from, any operating system, database, or file unless explicitly authorized by appropriate management and in compliance with institutional security policies, procedures, and standards. Additionally, software that can bypass, in any manner, approved security software or controls, may not be written or installed.

2.6 Personnel shall not disclose any information designated or otherwise marked as confidential or sensitive unless it is properly required in their job, or except as authorized in writing pursuant to security policies.

3. REVIEW AND RESPONSIBILITIES

Responsible Party (Reviewer): Chief Information Officer

Review: Biennial

Reprint of original policy statement. Signed original on file in the President's Office.