

## COMPUTER ACCOUNT ACCESS FORM

The following form must be completed and signed by new employees prior to receiving their network and email account information. A separate form must be completed for Banner and Fortis access.

Date: \_\_\_\_\_ D.O.B.\*: \_\_\_\_\_ Last 4 digits of SS#\* : \_\_\_\_\_

First Name\* : \_\_\_\_\_ Last Name\* : \_\_\_\_\_

Department Name\* : \_\_\_\_\_ Dept. Mgr. Name\* : \_\_\_\_\_

Room Number: \_\_\_\_\_ Phone Number: \_\_\_\_\_

Full-time Staff                      Part-time Staff                      Student-worker

Full-time Faculty                      Adjunct Faculty                      Other: \_\_\_\_\_

### COMPUTER ACCOUNTS

The following accounts are issued to all university employees:    Network Access:     Exchange Mailbox:

### DEPARTMENTAL AUTHORIZATION IS REQUIRED FOR THE FOLLOWING ACCOUNTS

**BANNER** – Student Records System. [Click here](#) to download a banner approval form.

**FORTIS** – Document Imaging System. [Click here](#) to download a fortis account form.

Or visit [www.uhd.edu/computing/forms.htm](http://www.uhd.edu/computing/forms.htm) to download forms.

### APPLICANT SIGNATURE

I have read the attached policy statements (**PS 08.A.04 and PS 08.A.05 and UHD Password Procedures**) and I agree to abide by them. I further agree that I will not disclose personal or confidential information obtained through the use of University of Houston-Downtown computer account(s).

By signing this form, I understand that by virtue of employment with the University of Houston-Downtown, I may have access to records that contain individually identifiable information, the disclosure of which is prohibited by the Family Educational Rights and Privacy Act of 1974, as Amended (FERPA).

I acknowledge that I fully understand that the intentional disclosure by me of this information to any unauthorized person could subject me to criminal and civil penalties imposed by law. I further acknowledge that such willful or unauthorized disclosure also violates policy of the University and could constitute just cause for disciplinary action including termination of my employment regardless of whether criminal or civil penalties are imposed.

**Applicant's Signature:** \_\_\_\_\_ **Date:** \_\_\_\_\_

Full-time staff account forms must be completed and submitted to Employment Services & Operation (910-S).

Account information will be distributed during the New Employee Orientation. All other employees can submit this form directly to Information Technology (700-S). Accounts issued to non full-time staff (part-time/student workers) expire two weeks into the subsequent semester. Accounts issued to adjunct faculties expire at the end of the next long semester.

**For IT Use: Date Received:** \_\_\_\_\_ **Call #:** \_\_\_\_\_

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.

Memo to: All UH - Downtown/PS Holders  
From: Max Castillo, President  
Subject: Academic Computing Services

UH - Downtown/PS 08.A.05  
Issue No. 1  
Effective date: 3/23/94  
Page 1 of 1

### **1. PURPOSE**

The purpose of this PS is to establish policies and procedures which govern Information Systems support services for academic computing.

### **2. POLICY/PROCEDURES**

2.1 Information Systems administers the central academic lab and publishes procedures and policies that govern the access and use of the lab. Information Systems may also administer or jointly operate with academic colleges a number of satellite labs on campus.

2.2 Requests for hardware, software or support resources may be referred by the director of academic computing to the appropriate committee for review and recommendation. This includes, but is not limited to, electronic classroom and satellite lab support, requests for additional support in the academic computing lab, new software and hardware installation, research support, additional training, new product review requests and additional resources to support curriculum changes.

2.3 Academic grant proposals which may result in significant information systems support must be reviewed by the Chief Information Officer and/or the Information Systems Steering Committee prior to processing. Information systems will assist the academic departments in incorporating procedures within their grant review process to notify the Chief Information Officer or the Information Systems Steering Committee of such proposals.

### **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.

University of Houston - Downtown

## Regulations for Using Academic Computing Facilities and Resources

The primary function of the Department of Academic Computing is to provide computing resources and user support for instructional activities at the University of Houston – Downtown (UHD). All users of academic computing facilities and resources are subject to the following regulations:

UHD students, faculty and staff are eligible to use academic computing facilities and resources. Access will not be granted to others without approval by the director of academic computing.

Users must present a valid UHD I.D. card when entering the Academic Computing Lab.

Lab users are expected to conduct themselves in a responsible and courteous manner while in the Academic Computing Lab.

Computing accounts are for use only by the person to whom the account has been issued by authorized computing personnel. A user may not disclose his/her password or allow other users to access his/her account.

Computers and resources in academic computing facilities are to be used for university-related purposes. They are not to be used for business or other profit-producing endeavors or for recreational purposes. Games are prohibited on all Academic Computing resources. This restriction does not apply to games and simulations used in conjunction with academic courses or research. The director of academic computing must receive written notice from the instructor of record in advance of such use.

Compromising the security of any computer or network or using university computing resources to engage in any illegal activity is strictly prohibited.

Each user is fully responsible for the activity of any account that has been assigned to him/her. If a user suspects that his/her account has been accessed by another user, the director of academic computing should be notified immediately.

Any changes to student accounts or access to any system must be requested by the respective faculty member.

Users may not write, use or have possession of programs that may be used to intimidate, harass, create an offensive environment for or invade the privacy of other users.

Users shall not represent themselves electronically as others.

Users shall not obstruct or disrupt the use of any computing system or network by another person or entity either on the UHD campus or elsewhere.

Users shall not, by any means, attempt to infiltrate a computing system or network either on the UHD campus or elsewhere.

All users of UHD's external network connections shall comply with the evolving "Acceptable Use" policies established by the external networks' governing bodies. Copies of policies relating to commonly accessed external networks will be made available in the Academic Computing Lab.

Copying of copyrighted software is illegal and is prohibited in the Academic Computing facilities or elsewhere on campus.

UHD forbids, under any circumstances, the unauthorized reproduction of software or use of illegally obtained software. Using university equipment to make illegal copies of software is prohibited.

Lab users may bring licensed personal copies of software into the Academic Computing facilities but may not install software on any computer or network or alter any existing software. Proof of ownership may be requested of users who bring software into the facilities.

Manuals and software may be checked out for use in the lab only.

Users should not attempt to repair any malfunctioning equipment or software, but should report any such occurrences to academic computing personnel.

Smoking, eating or drinking is not permitted in academic computing facilities.

Reservations for general lab use are not normally required; however, a temporary reservation system will be adopted as needed.

Although Academic Computing will make efforts to provide a safe and problem-free computing environment, in no event will the university or the Department of Academic Computing be liable for loss of data, inconvenience or other tangible or perceived damage resulting from or relating to system failures, viruses, user negligence, or other occurrences.

Academic Computing reserves the right to amend these regulations at any time, giving seven days notice before the amendments are to take effect. Notice will consist of an announcement displayed as part of the system login procedure on the systems for which user accounts are assigned, posting of an announcement at the front desk of the Academic Computing Lab, and notification of the Academic Computing Committee and the Student Government Association. Use of Academic Computing resources after the effective date of the modified regulations constitutes acknowledgement of the new regulations.

Use of academic computing accounts and resources in violation of these regulations, UHD policy, or any federal, state, or local laws may result in revocation of the individual's account privileges or suspension of access to computing resources, and may subject the account holder to university disciplinary action and/or criminal prosecution.

I have read the regulations printed above and agree to abide by them.

---

Applicant' s Signature

---

Date

## **Examples of Misuse of Computing Resources or User Accounts**

Using a computer account that you are not authorized to use.  
Obtaining a password for or gaining access to a computer account or directory which has not been assigned to you by authorized computing personnel;

Using the campus network to gain unauthorized access to any computer system;

Knowingly performing an act which will interfere with the normal operation of computers, terminals, peripherals, or networks;

Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or place excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses, and worms;

Attempting to circumvent data protection schemes or uncover security loop holes;

Violating terms of applicable software licensing agreements or copyright laws;

Deliberately wasting computing resources;

Using electronic mail or other means to harass others;

Masking the identity of an account or machine;

Posting on electronic bulletin boards materials that violate existing laws or the University's policies;

Attempting to monitor or tamper with another user's electronic communications, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner,

Damaging or stealing university-owned equipment or software;

Causing the display of false system messages;

Maliciously causing system slow-downs or rendering systems inoperable;

Changing, removing or destroying (or attempting the same) any data stored electronically without proper authorization;

Gaining or attempting to gain access to accounts without proper authorization;

Making copies of copyrighted or licensed software;

Using university computers for unauthorized private or commercial purposes.

*Activities will not be considered misuse when authorized by appropriate university computing officials for security or performance testing.*

# University of Houston-Downtown

## Network and Information System Password Procedure

### 1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of a user's data and ultimately lead to unauthorized access of UHD's network and information systems. As such, all UHD employees, students (including contractors and vendors with access to UHD systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

### 2.0 Purpose

The purpose of this procedure is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

### 3.0 Scope

The scope of this procedure includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that has access to the UHD network, or stores any non-public UHD information.

### 4.0 Policy

#### 4.1 General

- All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.
- All production system-level passwords must be part of the Information Technology Technical Services administered global password management database.
- All users are required to change their passwords at least once every 120 days. The recommended change interval is every 90 days.
- User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.
- All system-level passwords must conform to the password standards described below. All users should be strongly encouraged to follow similar standards for their passwords.

#### 4.2 Password Standards

##### A. General Password Construction Standards

Passwords are used for various purposes at UHD. Some of the more common uses include: user level accounts, web accounts, screen saver protection, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

- The password is short, alpha characters only and single case.
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, fantasy characters, etc.
  - Computer terms and names, commands, sites, companies, hardware, software.
  - The words "UHD", "DOWNTOWN", "HOUSTON" or any derivation.
  - Birthdays and other personal information such as addresses and phone numbers.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - Any of the above spelled backwards.
  - Any of the above preceded or followed by a digit (e.g., secret1, 1secret, 2004, 2005)

Strong passwords have the following characteristics:

- Contain both upper and lower case characters (e.g., a-z, A-Z)

- Have digits and punctuation characters as well as letters e.g., 0-9, !@#\$%^&\*()\_+|~-=\`{}[]:;'<>?,./)
- Are at least six to eight alphanumeric characters long.
- Are not words in any language, slang, dialect, jargon, etc.
- Are not based on personal information, names of family, etc.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

### **B. Password Protection Standards**

Do not use the same password for UHD accounts as for other non-UHD access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, don't use the same password for various UHD access needs. For example, select one password for the Engineering systems and a separate password for IT systems.

Do not share UHD passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential UHD information.

Here is a list of "don'ts":

- Don't reveal a password over the phone to ANYONE
- Don't reveal a password to the boss
- Don't talk about a password in front of others
- Don't hint at the format of a password (e.g., "my family name")
- Don't reveal a password on questionnaires or security forms
- Don't share a password with family members
- Don't reveal a password to co-workers while on vacation
- Don't create a password binder to store passwords

If someone demands a password, refer them to this document or have them call someone in Information Technology.

Do not use the "Remember Password" feature of applications (e.g., Eudora, Outlook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption.

Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months.

If an account or password is suspected to have been compromised, report the incident to Information Technology and change all passwords.

### **C. Application Development Standards**

Application developers must ensure their programs contain the following security precautions. Applications:

- should support authentication of individual users, not groups.
- should not store passwords in clear text or in any easily reversible form.
- should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

## **5.0 Enforcement**

Any employee found to have violated this policy may be subject to suspension of their UHD network and system access and/or disciplinary actions.