Guest Network Account Request Form

Applicant Information

Name: _____ Telephone Number: _____

E-mail Address: _____

Company Information

Company Name: _____ Telephone Number: _____

Address: _____ City: _____

State: _____ Zip: _____

DURATION OF VISIT - *Please indicate the exact dates you are requesting access.*	
Beginning Date: _____	End Date: _____

Applicant's Signature I have read the attached policy statements (PS 08.A.04 and PS 08.A.05) and I agree to abide by them.

_____ _____

Signature of Applicant **Date**

Sponsor Information

Name: _____ Telephone Number: _____

Department: _____ Room Number: _____

E-mail Address: _____

STATUS: Please select one

☐ Full-time Faculty ☐ Part-time Faculty ☐ Full-time Staff

Sponsor's Signature Sign and date.

_____ _____

Signature of Sponsor **Date**

Please submit this form to the Help Desk in Academic 700. For assistance or additional information regarding your request, please contact our Help Desk at 713-221-8031, x3000, or help@uhd.edu.

Memo To: All UH-Downtown/PS Holders

From: William Flores, President

Subject: Computer Access, Security, and Use Policy

1. PURPOSE

This PS defines the policy for all users of the University of Houston-Downtown (UHD) computers, computing systems, computer resources, software components, and/or other related applications (hereinafter collectively referred to as "Computing Systems").

2. DEFINITIONS

2.1 Incidental personal use: Incidental personal use is defined as occasional personal use of minimal time and duration, which results in no additional cost to UHD.

3. POLICY

3.1 The University of Houston-Downtown Computing Systems exist to provide computing services to the UHD community in support of instruction, research, and other educational and work-related activities within its mission.

3.2 UHD Computing Systems should be used in a manner that is consistent with the instruction, research, and other educational activities within UHD's mission.

3.3 Incidental personal use of UHD's Computing Systems is an exception to this general rule. Incidental use of UHD's Computing Systems must not interfere with assigned job duties and responsibilities or be in violation of existing University of Houston System or UHD policies, or applicable state or federal law.

3.4 Users have the responsibility to use UHD's Computing Systems in an effective, efficient, ethical, and lawful manner. The ethical and legal standards that are to be maintained are derived directly from standards of common sense and common decency that apply to the use of any public resource.

3.5 The University of Houston-Downtown (UHD) must adhere to the copyright laws concerning computer software. Unauthorized use or duplication of software is a federal crime. 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 Technology will maintain a list of federal and state laws which govern legal use of hardware and software.

3.6 UHD's Computing Systems are a state resource and should not be used by unauthorized personnel or for personal or corporate profit. Access to and use of computing resources is restricted to appropriately identified, authenticated, and authorized users.

3.7 All identification, passwords, 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.

3.8 Wireless access at UHD must be managed by and coordinated through UHD's Department of Information Technology to insure compliance with appropriate security standards and requirements defined by the state. Users must adhere to UHD's Wireless Access Guidelines, Exhibit A.

3.9 As a condition of use of UHD's Computing Systems, the user agrees to:

3.9.1 Respect the intended usage for which access was granted. Examples of inappropriate use may include the use of UHD's Computing Systems for purely recreational purposes, the production of output that is unrelated to the objectives of the project, and in general, the use of computers simply to use computing resources. Inappropriate use may also include engaging in deliberately wasteful practices such as unnecessarily printing, downloading, or transmitting large files.

3.9.2 Respect the rights of other users. For example, users should not use UHD's Computing Systems in a manner that interferes with the efficiency and productivity of other users.

3.9.3 Exercise discretion and best judgment in deciding what to include in or attach to an email and to whom it should be sent. Emails sent, received or stored on computers owned, leased or administered by UHD may be subject to required public disclosure under the Texas Public Information Act.

3.9.4 Exercise discretion and best judgment when sending unsolicited e-mails. Sending unsolicited emails that are not work related may be a distraction to the recipient and could serve as a depletion of UHD resources. Additionally, emailing unsolicited or unwelcome messages could, in certain circumstances, be considered a violation of UHD policy or even a violation of law.

3.9.5 Implement appropriate security measures for using University Computing Systems and handling university data. Users may not physically remove confidential or sensitive university-owned data from on-site university computing systems without the expressed approval of the application/data owner. (Storage of sensitive or confidential data on laptops or other portable media devices should be avoided.)

3.9.6 Maintain appropriate discretion in handling university-owned data. Users of university messaging systems should be aware that e-mail and other messaging systems are not secure forms of communication by default. Sensitive or and/or confidential information including social security numbers, payment card numbers and other forms of confidential information should not be distributed via e-mail, instant messaging, chat, or other messaging tools, or accessed over unencrypted wireless networks.

3.9.7 Abide by all other applicable University of Houston System and UHD policies and procedures related to the use, maintenance, and/or security of UHD's Computing Systems. Such policies include, but are not limited to, applicable University of Houston System Administrative Memoranda, UHD Policy Statements, and UHD Information Technology policies such as the UHD Information Security Handbook.

4. PROCEDURES

4.1 Messages sent to all UHD e-mail users **(DT_All_Users),** require vice presidential level (or designee) approval.

4.2 When responding to messages, users should exercise caution before selecting the Reply All option. ***Reply All*** should not be used without vice presidential level (or designee) approval when responding to messages sent to all UHD users **(DT_All_Users)**.

4.3 Ongoing or serious problems regarding electronic mail should be reported to the Vice President for Employment Services and Operations.

4.4 Users are strictly prohibited from sending confidential or sensitive information, including an individual's name in conjunction with restricted personal information, such as an individual's social security number or other data protected under state or federal law (e.g. financial, medical or student data) via e-mail, instant messaging, chat, or other messaging tools unless the data is encrypted.

4.5 Users must adhere to UHD's Wireless Access Guidelines, Exhibit A. (Temporary wireless access for guests is addressed in the Wireless Access Guidelines, Exhibit A.)

4.6 User access reviews must be conducted at least annually for Major Enterprise Application Systems (e.g. the Student Records, Financial Aid, Human Resources, and Finance Systems). Access reviews are the responsibility of the Application Owner in coordination with the Application Custodian.

4.7 A copy of this policy and PS 08.A.05, Academic Computing Services, is distributed with all new computer account requests.

5. EXHIBITS

Exhibit A: Wireless Access Guidelines

6. REVIEW PROCESS

Responsible Party: (Reviewer): Chief Information Officer

Review: Every three years on or before May 1st.

Signed original on file in Employment Services and Operations.

7. POLICY HISTORY

This is the first issue of this policy.

8. REFERENCES

University of Houston System Administrative Memoranda
UHD Policy Statements
UHD Information Security Website
Texas Public Information Act
PS 08.A.05

Exhibit A
PS 08.A.04

UNIVERSITY OF HOUSTON-DOWNTOWN

WIRELESS ACCESS GUIDELINES

Wireless access at UHD must be managed by and coordinated through UHD's Department of Information Technology to insure compliance with appropriate security standards and requirements defined by the state.

Users may not install wireless access points in UHD facilities without formal approval and oversight by UHD's IT Department.

Managing and Installing Wireless Access in UHD Facilities is the responsibility of Information Technology's Technical Services unit.

SSID values must be changed from the manufacturer default setting.

SSID names are defined by the Technical Services unit and must be coordinated with UHD User Support.

Encryption of at least 128 bit must be enabled (WPA or WEP) on UHD's Wireless networks.

UHD IT will conduct regular site reviews to detect unauthorized wireless access points and report and/or remove them as appropriate.

Wireless administration of access points must be administered from a wired connection. Wireless administration capabilities of access points must be disabled if applicable.

Users may not transmit confidential information via a wireless connection to, or from a portable computing device unless encryption methods, such as a Virtual Private network (VPN), Wi-Fi Protected Access, or other secure encryption protocols that meet appropriate protection or certification standards, are used to protect the information.

Guests who need access to the UHD wireless network may contact the UHD Help Desk (713-221-8031 or help@uhd.edu) to arrange for a temporary account (requires sponsorship by a UHD department representative). (See Wireless Network Account Request Form)

Memo To: All UH-Downtown/PS Holders

From: William Flores, President

Subject: Academic Computing Services

1. PURPOSE

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

2. DEFINITIONS

There are no definitions associated with this policy.

3. POLICY

3.1 Information Technology administers the central academic computing labs and publishes procedures and policies that govern the access and use of the labs. Information Systems may also administer or jointly operate with academic colleges a number of satellite labs on campus. Regulations for Using Academic Computing Facilities and Resources may be found in the References section of this policy.

3.2 Requests for hardware, software or support resources may be referred to the Director of User Support Services 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.

3.3 Academic grant proposals which may result in significant information systems support must be reviewed by the Chief Information Officer. Information Technology will assist the academic departments in incorporating procedures within their grant review process to notify the Chief Information Officer.

4. PROCEDURES

4.1 A copy of this policy and PS 08.A.04, Computer Access, Security, and Use Policy, are distributed with all new computer account requests.

5. EXHIBITS

There are no exhibits associated with this policy.

6. REVIEW PROCESS

Responsible Party: (Reviewer): Chief Information Officer

Review: Every three years on or before May 1st.

Signed original on file in Employment Services and Operations.

7. POLICY HISTORY

Issue #1: 03/23/94

8. REFERENCES

Regulations for Using Academic Computing Facilities and Resources
PS 08.A.04

University of Houston – Downtown

Regulations for Using Academic Computing Facilities and Resources

The primary function of the Academic Computing Services 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 manager of student technology services.

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 manager of student technology services 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 manager of student technology services 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.

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.

Eating or drinking is not permitted in academic computing facilities unless otherwise designated.

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 Academic Computing Services 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.

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.

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 (i.e. playing computer games, etc.);

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 Procedures

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 Password Procedures

4.1 General
- 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 90 days. Please note that the university's password standards enforce password history by prohibiting the reuse of old passwords.
- 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 UHD user account passwords must conform to the password standards described below.

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.

UHD requires that all users to establish strong passwords in order to gain UHD system access. As such, the university has put in to place strengthening attributes that all passwords must possess in order to be valid.

System policies require that all new or changed passwords meet the following standards:

- include a minimum of **eight (8)** characters; and
- contain a character from at least **three (3) out of the following four (4)** character sets:

    1) capital letter (A – Z)
    2) lower case letter (a – z)
    3) digit (0 - 9)
    4) special character (such as !, $, #, %)

- Must NOT contain more than two (2) consecutive characters from the authorized users name (e.g., John George Doe) or User Name (e.g., DoeJ1)

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)

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 best practice "don'ts" for your reference:

- 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.
- Don't use the "Remember Password" feature of applications.
- Don't store passwords in a file on ANY computer system (including PDAs) without encryption.

IMPORTANT: UHD, or other legitimate entities (including banks, airline companies, PayPal, eBay and the IRS) WOULD NEVER request that you submit personal information such as passwords, social security numbers, birthdates, etc. by replying to an e-mail message. It is also important to avoid visiting links or opening attachments associated with any messages of this type.

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

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

5.0 Enforcement

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