University of Houston-Downtown
Division of Information Technology

Vendor Computer Account Request Form

Last Revised 10/24/2005

Today's Date: ____/____/_____ For IT office use: Received: _____/_____/_____ Help Desk _____

Name (please print): _____ Title: _____

Company: _____ Phone Number (_____)_____

On which Sever does the Vendor need access to? _____

What Application is the Vendor working on? _____

Will the Vendor require remote access to the server?:_____

If Yes, what IP will the vendor be connecting from:_____

Begin Time/Date: _____ **End Time/Date:**_____

(If no end date is given, the vendor account will expire at the end of the business day)

_____	_____	_____
IT Contact (Print)	IT Contact (Signature)	Date

Vendors must comply with all applicable UHD policies, practice standards and agreements, including, but not limited to:

Information Systems Security and Access Policy
Network and Information System Password Procedure

Applicant's Signature is required.

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). (Note: contractors and vendors who use university computer account(s) are expected to treat all information obtained through the use of these accounts as confidential unless otherwise authorized by the university.)

Applicant's Signature: _____ **Date:** _____

Please return this form to the Division of Information Technology (700-South).

Account information will be sent directly to the applicant.
Information Technology Phone (713) 221-8031 Fax (713) 221-8684

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 ithelp@uhd.edu) to arrange for a temporary account (requires sponsorship by a UHD department representative). (See Wireless Network Account Request Form)

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.