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.

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 emails. 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 email 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 email, 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 email 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 email 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 email, instant messaging, chat, or other messaging tools unless the data is encrypted.

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

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

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: 05/01/10

8. REFERENCES

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