



University of Connecticut Health Center

POLICY NUMBER 2007-07

August 28, 2007

POLICY: Information Technology Computer Use Policy

PURPOSE:

This document establishes essential guidelines, protocols and standards of behavior for the use of computing resources at the University of Connecticut Health Center. As employees of the Health Center, we are also bound by applicable Federal laws and statutes of the State of Connecticut. (See State statutes at <http://www.ct.gov/doit/cwp/view.asp?a=1245&Q=314686>)

SCOPE AND APPLICABILITY:

This policy applies to all UCHC faculty, staff, and students and all other individuals granted access to UCHC computing resources. The policy applies to all computing and networking equipment and software owned, leased, operated, or contracted by UCHC including, but not limited to, personal computers, drives, printers, scanners, network's, video and audio recorders, cameras, photocopiers, telephones, PDA's and other related devices. Networks include, but are not limited to, all voice, video and data systems, including the UCHC Intranet and the Internet, both wired and wireless.

POLICY STATEMENT:

1.0 Privacy/Confidentiality

- 1.1 Information Technology makes every effort to ensure the integrity of individual and institutional information stored on UCHC systems, although absolute security and privacy cannot be guaranteed. Individuals with access to UCHC computing resources are expected to respect the privacy of the individuals whose information they can access, and to use reasonable and prudent methods to preserve the integrity and privacy of information within their control. Specific UCHC policies relative to HIPAA Privacy and Security requirements can be found under "UConn Health Center Policies" on the UCHC website.
- 1.2 While UCHC intends to provide a reasonable level of privacy, users should be aware that UCHC retains the right to access UCHC owned resources when necessary and appropriate. Information stored on UCHC systems may also be subject to disclosure upon request pursuant to various state and federal laws

including the Freedom of Information Act. UCHC does not, however, actively monitor the information content exchanged or stored on its systems.

- 1.3 In general, the content of user-files and network transmissions will not be viewed, monitored, altered, or disclosed without the expressed permission of the user, except in the following circumstances:
 - When required by Federal or State law, regulation, policy, rule, or directive (e.g. court order), electronic files will be made accessible.
 - When required by a criminal investigation, access to electronic files will be provided.
- 1.4 When there is no compelling external authority, and no criminal investigation to be supported, access to password protected files without the owner's permission can only be granted if there is:
 - A legitimate UCHC mission-related need for information, **or**
 - A credible allegation, or actual evidence, of some violation of UCHC or University of Connecticut policy, **and**
 - The specific procedures outlined below are followed, which require written approval by the senior officer of the Health Center (Executive Vice President for Health Affairs) or his/her designee.
- 1.5 Access to password-protected files without the owner's permission requires the submission of a completed "Application for Obtaining Password Protected Information" form to the Executive Vice President. The form must be signed by the requestor and the Director of Labor Relations, Human Resources, before forwarding to the Executive Vice President for Health Affairs. A copy of the form is at <http://itweb.uchc.edu/MainIT/Computing-Pol.htm> (Contact IT Security for guidance.)
- 1.6 If the Executive Vice President approves the request, the completed form is presented to the CIO, who then executes the file search described and authorized on the form and releases the results to the authorized requestor.
- 1.7 This policy does not include those IT procedures routinely performed in support of the network and individual computers/servers. The expectation is that file content will only rarely be exposed during such procedures and IT personnel will make every effort to ignore any exposed content.

2.0 General Usage Policy: Intended Purposes Only

The University of Connecticut Health Center provides information technology resources to enable faculty, students and staff to accomplish work that is the mission of UCHC. UCHC computing and networking equipment and software are to be used for UCHC business only. Computing resources are not to be used to conduct private business or commercial activities or any other illegal or prohibited activity such as unlicensed and illegal copying or distribution of

software that violates federal or state statues or regulations or are in conflict with UCHC's status as a public institution.

3.0 Authorized Access Only

Individuals with authorized access to UCHC systems may not intentionally seek or provide information or access to technology resources to one who is not authorized, nor assist others in doing so, nor attempt to subvert or circumvent UCHC Systems' Security Measures, nor use UCHC technology to subvert or circumvent other systems security measures for any purpose.

4.0 Harrassment

UCHC respects the First Amendment rights of freedom of speech and does not restrict the content of electronic mail or web pages. However, no member of the UCHC community may, under any circumstances, violate UCHC policies including, but not limited to, Prohibition of Sexual Harassment, UCHC Rules of Conduct, UCHC Code of Conduct, or the Affirmative Action, Non-Discrimination, and Equal Opportunity policy, through use of UCHC-owned computers, networks or other technological resources.

5.0 Obstructing, Disrupting or Otherwise Interfering with Activities of Others

UCHC prohibits individuals with access to UCHC technology resources from engaging in any activity that intentionally disrupts or damages software, hardware or other technological-related resources belonging to UCHC, compromising another individual's ability to use technological-related resources.

6.0 Reporting Potential Abuses

Members of the UCHC community who have observed, have knowledge of, or been the victim of, any unauthorized access attempts or other improper usage of UCHC technological resources should report such violations.

7.0 Policy Violation

Violations of this policy will result in appropriate disciplinary measures in accordance with UCHC HR policies, Rules of Conduct, applicable collective bargaining agreements, and the applicable Student Conduct Code.

Sandra Armstrong (signed)

9/7/07

Chief Information Officer

Date

Peter Deckers, M.D. (signed)

9/11/07

Executive Vice President for Health Affairs

Date

New Policy: August 28, 2007