UCONN HEALTH

POLICY NUMBER 2007-07

July 12, 2011

POLICY: INFORMATION TECHNOLOGY COMPUTER/ELECTRONIC RESOURCE USE POLICY

PURPOSE:
This document establishes essential guidelines, protocols and standards of behavior for the use of electronic resources at UConn Health. Employees of UConn Health are also bound by applicable Federal laws and statutes of the State of Connecticut.

DEFINITIONS:
Electronic resources are computing and telecommunications devices that can execute programs or store data; examples of which may include, but are not limited to: computers, mobile computing devices, smartphones, and storage devices (USB or otherwise connected).

SCOPE AND APPLICABILITY:
This policy applies to all UConn Health faculty, staff, and students and all other individuals granted access to UConn Health electronic resources. The policy applies to all computing and networking equipment and software owned, leased, operated, or contracted by UConn Health.

POLICY STATEMENT:
Privacy/Confidentiality

1. Information Technology makes every effort to ensure the integrity of individual and institutional information stored on UConn Health systems, although absolute security and privacy cannot be guaranteed. Individuals with access to UConn Health electronic 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 policies relative to Information Privacy and Security requirements can be found under "UConn Health Policies" on the UConn Health website.

2. While UConn Health intends to provide a reasonable level of privacy, users should be aware that UConn Health retains the right to access UConn Health owned resources when necessary and appropriate. Information stored on UConn Health systems may also be subject to disclosure upon request pursuant to various state and federal laws including the Freedom of Information Act. UConn Health does not, however, actively monitor the information content exchanged or stored on its systems.

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.

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 UConn Health mission-related need for information, **or**
    - A credible allegation, or actual evidence, of some violation of UConn Health or University of Connecticut policy, **and**
    - The specific procedures outlined below are followed, which require written approval by the Senior Officer of UConn Health (Vice President for Health Affairs) or his/her designee.

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 Vice President for Health Affairs. The form must be signed by the Requestor, the subject's immediate Supervisor, and the Director of Labor Relations, before forwarding to the Vice President for Health Affairs. If there is a conflict of interest for any of the signatories, their next level manager will provide approval by signing. A copy of the form follows this policy (Contact IT Security for guidance.)

6. If the Vice President for Health Affairs 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.

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.

General Usage Policy: Intended Purposes Only

UConn Health provides electronic resources to enable faculty, students and staff to accomplish work that is the mission of UConn Health. UConn Health computing and networking equipment and software are to be used for UConn Health business only. Electronic 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 UConn Health's status as a public institution.

Authorized Access Only

Individuals with authorized access to UConn Health 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 UConn Health Systems' Security Measures, nor use UConn Health technology to subvert or circumvent other systems security measures for any purpose.

Harassment

UConn Health 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 UConn Health community may, under any circumstances, violate UConn Health policies including, but not limited to, Prohibition of Sexual Harassment, UConn Health Rules of Conduct, UConn Health Code of Conduct, or the Affirmative Action, Non-Discrimination, and Equal Opportunity policy, through use of UConn Health-owned computers, networks or other technological resources.

Obstructing, Disrupting or Otherwise Interfering with Activities of Others

UConn Health prohibits individuals with access to UConn Health electronic resources from engaging in any activity that intentionally disrupts or damages software, hardware or other resources belonging to UConn Health, compromising another individual's ability to use any resources.

Reporting Potential Abuses

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

Policy Violation

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

Attachment:

Application for Obtaining Password Protected Information Form

Sandra Armstrong (Signed) 8/22/11

Chief Information Officer **Date**

Philip Austin (Signed) 8/23/11

Vice President for Health Affairs **Date**

Revised: 08/28/07, 07/12/11