A. INTRODUCTION

Over the past two years, Internet-borne computer viruses, hacking attempts, and other related cyber-attacks have become more frequent and more severe. The most effective way to secure electronic assets is to adopt additional computing policies in the area of security. Adopting tighter computer security policies may introduce some inconvenience and process changes, but the payoff will be better protection of electronic resources for individuals, departments, and the campus as a whole.

UCHSC information technology providers are responsible for managing and protecting the information technology resources under their jurisdiction as well as creating and enforcing policies regarding provision and use of the respective information technology resources. The use of computing and networking resources of the UCHSC is a privilege
and as such, any individual who uses the information technology resources of the UCHSC is responsible for making use of these resources in an efficient, ethical, legal, and secure manner.

This policy applies to all users of the UCHSC internal data network who are connected through either a direct physical connection or connected via wireless connections, campus modem lines, DSL service, cable modems, over the Internet, or by other means.

B. DEFINITIONS

Users of the UCHSC internal network refers to any individuals and/or electronic devices that are connected to the UCHSC Campus comp using infrastructure that interconnects computers, networking equipment, printers, personal digital assistants, and electronic devices for the purpose of data or information exchange.

IT – is an abbreviation for information systems

IS – is an abbreviation for information technology

Users of the UCHSC internal network – is a password that is not readily decipherable and usually consists of symbols/characters, letters, and/or numbers that will allow a user to gain access to the UCHSC internal network.

UCHSC Department – is the centralized service unit that provides data networking, e-mail, file server, telephone, and other information technology support services for the UCHSC campus

C. POLICY STATEMENTS

1. General

The IT resources of the UCHSC should be used and managed consistent with the purpose for which the IT resources were intended and in a manner that is consistent with the UCHSC mission of teaching, conducting research, and providing health care and public service.

All activities inconsistent with these objectives or that could be construed to constitute a conflict of interest or commitment is considered to be inappropriate and may jeopardize the user’s privilege of using IT resources. To ensure the protection of IT resources, UCHSC reserves the right to probe and monitor computing activities on any and all devices connected to the UCHSC network to ensure they are operating in compliance with this policy. In addition, UCHSC may withdraw a user’s privileges when violations of this policy occur.

2. Conditions for Use of UCHISC IT Resources
a. The use of campus standard products for anti-virus protection is mandatory and exceptions are only allowed if the UCHSC IS Department authorizes exclusions due to unique and extraordinary circumstances.

b. UCHSC IS will manage an automated process of anti-virus software distribution and reporting of virus activity for the campus.

c. UCHSC IS will retain login rights on campus desktops and servers in order to update anti-virus software and respond to emergencies.

d. Web servers should only be operated when necessary to serve the missions of the University. In order to reduce the threat of computer viruses and other attacks, they must be configured securely and maintained on an ongoing basis. To ensure compliance with these requirements, all campus web servers must be registered with and approved by UCHSC IS.

e. If computers share disk drive space over the campus network without password protection, it leaves the campus open to viruses and other attacks. As a result, this method of sharing disk space is now prohibited.

f. All suspected policy violations; system intrusions, virus infestations and other conditions, which might jeopardize UCHSC IT resources, should be immediately reported to the Director of Information Systems Security (phone 303-724-0440).

3. **Non-compliance with Policies**

a. UCHSC IS will identify non-compliant systems through network monitoring or other means.

b. UCHSC IS will follow up with communications to owners of non-compliant passwords.
   i. Direct telephone or e-mail contact with system owner
   ii. Contact with departmental IT staff
   iii. Escalation via departmental administrative channels

c. Remedies will take the form of one of the following options:
   i. Either, install the software and configure systems as needed; or
   ii. The IS department will authorize a written exclusion from this policy; or,
   iii. The account(s) will be removed from the campus network.

Notes

1. Dates of official enactment and amendments:
   November 5, 2001: Adopted by Provost

2. History:
   September 6, 2018: Modified to reflect a 2018 Campus-wide effort to recast and
revitalize Campus policy sites into a standardized and more coherent set of chaptered policy statement organized around the several operational divisions of the university. Article links, formatting, and University branding updated by the Provost’s office. July 1, 2019: Reviewed as part of the spring 2019 semi-annual review process. This campus-level IT security policy is redundant with CU system APS 6005: IT Security Program, which was developed in collaboration with the other CU campus Information Security Officers.

3. Initial Policy Effective Date:
   November 5, 2001

4. Cross References/Appendix:
   - University Policy Framework and Hierarchy;
   - University of Colorado Administrative Policy Statement “Copying Computer Software”
   - University of Colorado Administrative Policy Statement “Use of Electronic Mail”
   - University of Colorado Health Sciences Center Administrative Policy Statement “Use of Information Technology”