UNIVERSITY of DENVER	**UNIVERSITY OF DENVER** **POLICY MANUAL** **USE OF COMPUTER AND NETWORK SYSTEMS**

Responsible Department: Office of Information Technology **Recommended By:** VC for Information Technology and Chief Information Security Officer, SVC Business and Financial Affairs **Approved By:** Chancellor	**Policy Number** IT 13.10.010	**Effective Date** 9/__/2021

I. INTRODUCTION

The University of Denver maintains access to local, national, and international networks for the purpose of supporting its fundamental activities of instruction, research, and administration.

II. POLICY OVERVIEW

A. This policy applies to all persons accessing computer or network resources through any network or University facility.

B. Computer, system or network users **must**:

1. Use the computer, system or network in ways that do not interfere with or disrupt the normal operation of the computer, system or network;
2. Respect the rights of other users, including their rights as set forth in other University policies for students, faculty, and staff; these rights include but are not limited to privacy, freedom from harassment, and freedom of expression;
3. Know and obey all University and Information Technology policies established for the system and networks they access;
4. Comply with applicable laws and terms of applicable contracts and license agreements; and
5. Safeguard equipment entrusted to them.

C. **Users** of the University computers, systems or networks **may not**:

1. Share accounts, usernames or passwords
2. Attempt to view or intercept data or network traffic not intended for their viewing or use;
3. View, copy, disclose, or modify any files or data that does not belong to them, or to which they do not have specific permission;
4. Use computing or network resources to harass, threaten, or otherwise

cause harm to others;

5. Use the University's computing resources for commercial or personal purposes not related to the University's business operations, academic, research, and scholarly pursuits;
6. Use any IT systems in a way which suggests University endorsement of any political party, candidate, or ballot initiative (this includes e-mailing political messages to any list service maintained by the University which is not explicitly purposed for the posting of political messages);
7. Interfere with the proper functioning of the University wired or wireless networks (*See* Policy IT 13.10.014 - *Wireless Access;* Policy IT 2.30.066 – *Mobile Device Use*, and Policy IT 13.10.030 - *Network Security*); and
8. Use University IT systems to distribute, produce, publish, and/or sell obscene or illegal content.

D. The University does not monitor or generally restrict the content of material traversing the University's networks or stored on University managed or contracted systems and devices. The University reserves the right to remove or limit access to material posted on University-owned or administered systems and networks when University policies, contractual obligations, or state or federal laws are violated.

E. The University provides computers, software, and network equipment for use by the University community. The University retains ownership and reserves the right to add, remove, upgrade, and replace hardware or software on those systems as deemed necessary by Information Technology.

III. PROCESS OVERVIEW

A. User Responsibilities

1. *Copyrights and Licenses*. Users must respect copyrights and licenses to software and other on-line information.

    a. **Copying:** All software protected by copyright must not be copied except as specifically stipulated by the owner of the copyright or otherwise permitted by copyright law.
    b. **Number of Simultaneous Users:** The number and distribution of copies must be handled in such a way that the number of simultaneous users does not exceed the number of original copies purchased, unless otherwise stipulated in the purchase contract.
    c. **Copyrights:** In addition to software, all other copyrighted information (text, images, icons, programs, etc.) must be used in conformance with applicable law. Legitimately, copied material must be properly attributed. Plagiarism of computer information is subject to the same sanctions as apply to plagiarism in any other media.

d. **Digital Millennium Copyright Act:** The University complies with the **Digital Millennium Copyright Act**. The University may terminate the network access of users who are found to repeatedly infringe the copyright of others and may take other disciplinary measures it deems appropriate.

2. *Integrity of Information Resources***.** Users must respect the integrity of information resources.

   a. **Modification or Removal of Equipment:** Computer equipment, software, or peripherals owned by others must not be modified or removed without proper authorization.
   b. **Encroaching on Others' Access and Use of University Facilities:** Users must not encroach on others' access and use of the University's network and computers. This includes but is not limited to: (i) sending unsolicited bulk electronic mail or distributing unsolicited material though group communication channels; (ii) Sending chain-letters; (iii) Excessive printing; (iv) Using excessive network bandwidth; (v) Running grossly inefficient programs when efficient alternatives are available; (vi) Modifying system facilities, operating systems, or disk partitions without proper authorization; (vii) Attempting to access private information without proper authorization; (viii) Attempting to crash or tie up University computers or networks; and (ix) Damaging or vandalizing University computing facilities, equipment, software or computer files.
   c. **Virus Protection:** All vulnerable computers connected to the University network must be protected by up-to-date anti-virus software.
   d. **Software Requirements:** Computers with grossly outdated or inherently insecure software may not be connected to the University network.
   e. **Spyware:** Software or hardware that monitors web browsing, keyboard use or related activities must not be installed on University computers. This restriction is not intended to limit in any way the University's right to monitor any and all hardware or software owned by the University, or connected to the University network, for the purposes of preventing or investigating improper or illegal use of University systems, or preventing or investigating system problems or efficiencies.
   f. **Unauthorized Network Connections:** Only officially assigned Internet Protocol (IP) numbers may be used for equipment connected to the University's data network. Use of unassigned static IP numbers is prohibited. The Director of Network Operations within the Information Technology division must approve any requests for using IP addresses not already assigned by the IT Operations team.
   g. **Falsified Message Sources:** Disguising or falsifying sources of electronic mail and other electronic communications with the intent of misleading, defrauding or harassing others is prohibited.

h. **Computer Registration:** Registering “head-less” computing equipment, such as gaming consoles, that require Internet connectivity using the University network is recommended.
i. **Unauthorized or Destructive Programs:** Users must not intentionally develop or use programs that disrupt others use of computers and networks, provide unauthorized access to private or restricted information, or damage software or hardware belonging to others.

3. *Unauthorized Access*: Users must refrain from seeking to gain unauthorized access to information resources or enabling unauthorized access.

   a. **Abuse of Computing Privileges:** Users must not access computers, computer software, computer data or information, or networks without proper authorization, or intentionally enable others to do so, regardless of whether the computer, software, data, information, or network in question is owned by the University.
   b. **Reporting Problems:** Any defects discovered in system accounting or system security must be reported to appropriate system administrators so that steps can be taken to investigate and solve the problem.
   c. **Password Protection:** Users who have been authorized to use password-protected accounts may be subject to both civil and criminal liability if they disclose passwords or otherwise make accounts available to others without permission of appropriate system administrators.

4. *Usage*.

   a. **Unlawful Messages.** Use of electronic communication facilities (such as e-mail, instant messaging, talk, chat rooms, threaded discussions or systems with similar functions) to send fraudulent, harassing, obscene, threatening, or other messages that are a violation of applicable federal, state or other law or University policy is prohibited.
   b. **Spam.** Use of the University's email system to send "spam" email is prohibited.
   c. **Bulk Email: T**he use of the University's email system as medium for the bulk distribution of information is discouraged. On rare occasions, email may be the best mechanism to distribute information to large segments of the University community. Approval of a University official with a ranking of vice chancellor or higher is required for messages sent to more than 200 people. Any bulk email/mass-communication must comply with the Bulk Email Policy.
   d. **Group Communication Channels:** Group communication channels such as mailing lists, threaded discussions, chat rooms, bulletin-boards, and courseware classrooms are generally set up for specific

purposes. Use of a group communications channel to distribute material inconsistent with the channel's purpose is not allowed.

e. All hosts on the University network should have a name that ends in **du.edu**. Any variations on a domain name (whether for a physical server or a virtual server) must be approved by the IT department.

f. **Content Filtering:** The general policy of the University is to avoid filtering content passed through the University network. However, content filtering may occur in the following circumstances:

i. The University will filter network traffic if it is legally required to do so.

ii. individual divisions that offer programs for children may elect to filter traffic to and from their sub-networks. These divisions will be responsible for content standards and filtering rules.

iii. The University may block e-mail from sites known to send or transport excessive amounts of unsolicited bulk e-mail.

iv. The University may scan e-mail for viruses, worms and other malicious programs. E-mail containing such programs may be refused either in whole or in part.

v. The University may block traffic likely to compromise the privacy of University information or the security and integrity of either internal or external networks.

vi. The University may prioritize traffic passing through its network based on assumptions about traffic types and their requirements for quality of service.

B. System Administrators' University Responsibilities

1. *Systems and Networks*. System administrators have the following responsibilities for systems and networks they administer:

a. Taking precautions against theft of or damage.

b. Protecting the integrity and privacy of personal, financial, and other confidential information stored on systems and networks they administer.

c. Executing all applicable hardware and software licensing agreements.

d. Following appropriate practices for security and disaster recovery.

e. Promulgating policies and procedures that govern services, access, and use of the systems they administer. At a minimum, this information should describe the data backup services, if any. A written document given to users or messages posted relevant web pages shall be considered adequate notice.

f. Reporting suspected legal violations, security threats or violations of University policy to appropriate University authorities. At a minimum, abuse@du.edu should be notified.

g. Cooperating with other system administrators, whether within or without the University, to find and correct problems caused by the use of systems under their control.

2. *Policy Enforcement*. System administrators are authorized to take reasonable actions to implement and enforce usage and service policies and provide for security.

3. *Suspension of Privileges*. System administrators may temporarily suspend access privileges if they believe it necessary to maintain the integrity of computer systems or networks. If legal violations, security threats, or violations of University policy are suspected, system managers should also inform appropriate University authorities. At a minimum, abuse@du.edu should be notified.

C. Computer Security Officer Responsibilities

1. *Policy Interpretation*. The Vice Chancellor for Information Technology shall be responsible for interpretation of this policy, resolution of problems and conflicts with local policies, and special situations.

2. *Policy Enforcement*. Where violations of this policy come to his or her attention, the Vice Chancellor for Information Technology is authorized to work with the appropriate administrative units to obtain compliance with this policy.

3. *Inspection and Monitoring***.** Only the University's Vice Chancellor for Information Technology or designate, can authorize the inspection of private data or monitoring of messages (including electronic mail) when there is reasonable cause to suspect improper use of computer or network resources.

The University's Vice Chancellor for Information Technology may also authorize general inspection and monitoring to assure the security and stability of the network and systems connected to it. This may include, but is not limited to, monitoring and inspection to support activities such as:

a. Assuring adequate quality of service for critical applications
b. Detecting unauthorized use of the network
c. Filtering content
d. preventing or investigating system problems or efficiencies
e. assessing security vulnerabilities of computers connected to the network
f. Preventing or investigating improper or illegal activities
g. Compiling usage statistics

D. Violations of This Policy

1. Suspected violations of this policy (e.g., any incidents involving the unauthorized access to, destruction of, or misuse of computing services by employees, faculty, or students) must be brought to the attention of the cognizant dean, director, or department head, and the University IT Security Office (abuse@du.edu). In the case of a criminal violation, the IT Security Office will notify the Office of Campus Safety. Violations by non-employees will be referred to the appropriate authorities. The Office of General should be contacted if assistance is needed to identify the appropriate authority.

2. The misuse, unauthorized access to, or destruction of University computing services in violation of applicable laws or University policy may result in sanctions, including but not limited to withdrawal of use privilege; disciplinary action up to and including expulsion from the University or discharge from a position; and legal prosecution.

3. Under some circumstances, as a result of investigations, subpoena or lawsuits, the University may be required by law to provide electronic or other records or other information related to those records or relating to use of information resources.

IV. DEFINITIONS

A. "System administrators" are individuals who have been designated to manage computing and networking systems in their divisions. System administrators have additional responsibilities to the University as a whole for the systems under their oversight, regardless of the policies of their divisions.

Revision Effective Date	**Purpose**
9/__/2021	*Aligning Policy with practice*