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 throu

h. **Computer Registration:** Registering - 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

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*.
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