Colorado Mesa University
Computer End-user Agreement and Notice of Computer Policies
("End-user Agreement")

IMPORTANT NOTICE of acceptable use of computing and network resources and acknowledgement of computer-related policies. The use of any University-owned computer or network signifies an acceptance of the following policies and adherence to computing information security best practices. (Please note: all University policies are published online in their entirety on the Colorado Mesa University website.)

Purpose: Colorado Mesa University ("University") provides students and employees ("End-users") the privilege to use its computers and network for the purposes of accessing software, information systems, and the Internet in support of the institution's mission. The University is responsible for the reliability and security of its computer systems and network and reserves the right to suspend user accounts or disconnect any computer or network-attached device, without warning, which poses a security or performance risk to the campus systems and network.

Computer Use Policy
University computers and networks are provided for the academic and administrative objectives of the University and shall be used in a manner consistent with the purpose for which they are provided. End-users are responsible for activities originating from their computers or network connection. End-users shall:

- Adhere to University policies and local, state and federal laws, including copyright law, and not use campus resources for any illegal activity or any prohibited uses outlined in this policy.
- Protect their CMU computer login username and password to protect University computers, network and information. This includes not sharing your passwords with anyone or for any reason.
- Follow information security best practices and support strong passwords, never leaving your computer logged on and unattended and never storing confidential information on mobile computing devices.
- Not impede the academic pursuits of other users.

Software Compliance: End-users shall use software in accordance with terms of license agreements and copyright laws. CMU does not have the right to reproduce software or related documentation without proper written authorization. The unauthorized copying or redistribution of copyrighted software is illegal. CMU reserves the right to impose disciplinary and/or legal action as deemed appropriate.

Prohibited Use includes, but is not limited to:
a) Sending or storing confidential information without authorization
b) Using University computers, networks, or resources for unauthorized commercial purposes
c) Using a computer account that you are not authorized to use
d) Illegally downloading and distributing copyrighted material, such as software, movies, music, and games, through the use of peer-to-peer (P2P) networking
e) Violating terms of software agreements or copyright laws
f) Using the University computers or networks to gain unauthorized access to any computer system

g) Utilize any personal computing device to gain unauthorized access to network resources.
h) Bypassing, disrupting, or disabling security controls or operation of the campus network or computer systems
i) Knowingly installing or spreading malicious software such as viruses and worms, or otherwise attempting to disrupt the performance of another computer system or network
j) Congesting the campus network and Internet bandwidth and hampering the productivity of other network users
k) Participating in any illegal activity including, but not limited to distributing pornography, harassing an individual or group, threatening the safety of persons, etc.
l) Monitoring, tampering with, or deleting another user's electronic communication or files without proper authorization.

Electronic Communications Policy

University-owned or operated electronic communication facilities are intended and shall be used solely for the academic and administrative objectives of the University and shall be used in a manner consistent with the purpose for which they are provided.

Policy and Plan to Combat Unauthorized Distribution of Copyrighted Material and Peer-to-Peer File Sharing

Copyright infringement and illegal use of peer-to-peer file sharing brought to the attention of Colorado Mesa University by copyright owners will result in the end-user's system and/or network account being suspended. The end-user's infringing activity may be reported to the CMU Student Conduct Officer, or the employee's supervisor and Human Resources as appropriate. Illegally copying or distributing copyrighted material may result in the loss of computer and network access privileges for up to 45 days, and in some cases these privileges may be lost indefinitely. University sanctions for copyright infractions are cumulative for the student's enrollment at CMU.

Information Security Best Practices

- Passwords must be 8 characters or more in length and be alphanumeric.
- Passwords should be memorized. Avoid writing your password down, and do not post your password on your computer or monitor.
- Do not share your password with anyone, for any reason.
- Passwords must be changed at least every 180 days.
- Do not leave any computer logged on and unattended. Always lock your workstation before your leave (ctrl-alt-del, Lock Workstation), and set your screen saver to activate and resume password protected.
- Never store confidential or private information on mobile media including laptops, USB drives, tablets, and smart phones.
- Do not connect any unauthorized devices to the campus network.
- Remember, network and computer security are everyone's responsibility. Please do your part to keep network and system accounts secure and electronically stored data safe. A strong password is a great way to start!

Please read carefully:

I understand that violating, or attempting to violate, any of the above-mentioned policies may result in disciplinary action, which may include revocation of my user account.
By selecting "I Accept," I agree to all the before mentioned University policies (in entirety), to follow all applicable local, state and federal laws, and to adhere to all computing and network security best practices as outlined above.

[I Accept]