UA Rich Mountain
Policy: Information Technology Acceptable Use
Version 2026.03.18 (UASP 280.1 & UASP 285.1)

Background

All users, including Students, Faculty, Staff, and Patrons, of UA Rich Mountain information systems are required to be familiar with and acknowledge receipt of this policy prior to gaining system access.

UA Rich Mountain is an institution of higher learning overseen by the government of the State of Arkansas. As such, most hardware and software associated with UA Rich Mountain are subject to the Governor's Policy Directive GPD-5 (1997). This directive states: "Use of any and all State-owned equipment and supplies shall be restricted to official state use only. Unauthorized or personal use of equipment of supplies may be grounds for dismissal." Certain hardware and software may belong to programs overseen by the federal government and may be subject to additional restrictions.

UA Rich Mountain information systems include all hardware and software that pass data in any form across the UA Rich Mountain local area network. Video conferencing, projection, and other audio-visual equipment are considered information systems subject to this policy.

UA Rich Mountain strives to provide users with the necessary tools for communication, research, collaboration, business operations, and other activities in furtherance of the UA Rich Mountain mission. UA Rich Mountain also acknowledges that limited personal use of information systems is inevitable and may be beneficial to both the individual and the institution. Therefore, it is helpful to understand both what constitutes acceptable use and those activities that are prohibited, regardless of whether personally owned or UA Rich Mountain equipment is used.

Purpose

This policy defines the appropriate use and procedures for using computer information systems on the University of Arkansas Community College Rich Mountain network, Physical or Virtual (VPN).

This policy applies to Students, Faculty, Staff, and Patrons, and any other user that utilizes the network or computing resources provided by University of Arkansas Community College Rich Mountain

Policy

This section does not address every situation of acceptable or unacceptable use of University of Arkansas Rich Mountain information systems, it does outline the personal responsibilities when UARM resources are utilized.

Any violation of UASP 285.1 or the University policy on use of technology resources shall be subject to the progressive discipline policy. Depending on the severity of the violation, disciplinary action may include suspension or termination.

Acceptable Use of Information Systems

- Accessing the network for work, educational, or related research and information gathering.

- Utility and applications software that accomplish tasks and fulfill job functions or educational requirements.
- Communication and collaboration between users and/or other appropriate entities.
- Access to the Internet for up-to-date information published by UA Rich Mountain, other state agencies, schools, various other providers of information.
- Activities or projects that support professional activities of users (i.e., electronic calendars, electronic scheduling of meetings, electronic prioritizing of tasks, using project management software, keeping electronic address books, and completion of work-related forms electronically).

Unacceptable Use of Information Systems

- Vandalizing equipment, software, or hardware.
- Interference with the security or operation of UA Rich Mountain information systems.
- Attempting to alter or gain unauthorized access to hardware or software.
- Sharing restricted access credentials with any other person or group, except authorized administrators.
- Attaching an unauthorized device to the UA Rich Mountain network, either wired or wirelessly.
- Installing unauthorized software on UA Rich Mountain equipment without the system administrator's consent.
- Playing networked games or games hosted on the Internet that are not directly related to educational work or approved esports activities.
- Using, submitting, publishing, displaying, or transmitting on the network or on any information system any information which:
    - Violates or infringes on the rights of any other person, including the right to privacy.
    - Contains defamatory, false, inaccurate, abusive, obscene, pornographic, profane, sexually oriented, threatening, racially offensive, or otherwise biased, discriminatory, or illegal material.
    - Inhibits other users from using the system or the efficiency of the information system.
    - Encourages the use of controlled substances or uses the system for the purpose of criminal intent.
    - Knowingly transmits or receives material, information, or software in violation of any local, state, or federal law.
    - Conducts any non-UA Rich Mountain-related fund raising or public relations activities.
    - Engages in any activity for personal financial or material gain, with or without a profit motive.
    - Views, downloads, or sends pornographic or other obscene materials.
    - Contains a payload with the intention to damage or infect another information system.
    - Intends to affect network availability or efficiency.
    - Uses the system for any illegal purpose or with criminal intent.
- Excessive use of social media or use that violates any provision above.
- Misrepresentation of identity or relationship to the University to obtain unauthorized access to computing resources.

User Responsibilities

Multi-factor Authentication

UA Rich Mountain requires Multi-factor Authentication (MFA) methods to access secure applications and services. MFA is considered a best practice in information security and may require the use of personal devices such as a mobile phone or tablet, or a device designated by the Computer Services Department, to receive authentication codes and/or one-time passwords for system access. The configuration and use of MFA is a basic requirement of employment/enrollment at UA Rich Mountain and is consistent with UA System requirements.

No user shall knowingly attempt to bypass or circumvent this requirement.

The first MFA device issued by the Computer Services Department to the employee will be free of charge, but replacement devices due to loss, destruction, or negligence will be a $50.00 charge.

Privacy of Information

University of Arkansas Rich Mountain users shall not place confidential information in computer systems without protecting it appropriately.

UA Rich Mountain reserves the right to monitor and/or log all network activity with or without notice, including UA Rich Mountain email and all website communications; therefore, unless otherwise stated, users should have no expectation of privacy or anonymity in the use of any information system. UA Rich Mountain does not routinely monitor user content.

UA Rich Mountain will never provide third parties with access to stored or transmitted information without the written consent of the sender and recipient except in exceptional circumstances, such as investigating illegal activity, misuse of the system, or resolving a technical problem.

Information leaving the UA Rich Mountain network may be subject to monitoring by governments, network carriers and other parties. Once this information leaves the campus network, access to it is no longer controlled by UA Rich Mountain.

Use of Protected Content or Resources

Users may not download material that is protected by U.S. copyright laws, subject to trademark restrictions, or encumbered by any other form of intellectual property rights protection unless it is legally allowed or falls under the Fair Use provision of copyright law.

Users may not upload, disseminate, or print material that infringes on copyright or any other intellectual property rights protection mechanism. UA Rich Mountain will comply with all takedown notices related to the Digital Millennium Copyright Act (DMCA) or similar legislation. UA Rich Mountain reserves the right to remove any item referenced in an infringement notice without the prior consent or notification of the user that uploaded or disseminated the item. Further, UA Rich Mountain will not be responsible for a user's legal defense or other costs associated with infringing material.

Enforcement and Penalties

UA Rich Mountain users are responsible for complying with this policy. Penalties for non-compliance

include, but are not limited to:

a. Suspension or usage restriction of information systems.
b. Internal disciplinary measures, including discharge from employment or enrollment.
c. Initiation of criminal or civil action, if appropriate.

UA Rich Mountain reserves the right to remove or block access to any information system, from any user or device, which adversely affects the availability or reliability of the information system or network without prior notification to the user or owner of the device.

Revision History

Version	Published	Author	Description
2005.02.11	2005.02.11	Mark Barton	Original
2020.07.13	2020.07.14	Chris Masters	Revision
2023.01.11	2023.01.27	Bryan Carnahan	Revision
2024.01.16	2024.02.6	Bryan Carnahan	Update
2024.05.16	2024.05.16	Bryan Carnahan	Update
2026.03.18	2026.03.18	Bryan Carnahan	Update