**MOUNTWEST COMMUNITY & TECHNICAL COLLEGE**
**BOARD OF GOVERNORS**
**Policy No. I - 1**

**INFORMATION TECHNOLOGY ACCEPTABLE USE**

Authority: W. Va. Code §18B-1-6

Passage Date: November 22, 2021

Effective Date: December 22, 2021

Last Revised Date: June 5, 2025

## Purpose and Scope

A trusted and effective Information Technology environment is vital to the mission of the College. College Technology Resources are provided for College-related purposes, including support for educational instruction and learning, community & public service missions, its administrative functions, and student life activities.

The purpose of this Policy is to establish the rules that govern the use of the devices and information systems at Mountwest Community & Technical College (College) to ensure both the protection of College Data and compliance with applicable laws and regulations.

## I. Applicability

1.1. This Policy applies to all individuals (Users) using College Technology Resources, regardless of affiliation and irrespective of whether these resources are accessed on-campus or from remote locations.

1.2. "College Technology Resources" in this document means the Campus Network, Campus-owned hardware, software, devices, and communications equipment, technology facilities, and other relevant hardware and software items, as well as personnel tasked with the planning, implementation, and support of technology.

## II. EXPECTATIONS OF AUTHORIZED INDIVIDUALS, APPROPRIATE USE

2.1. Adhere to, and maintain all College Technology Resources according to, established College policies, standards, and procedures.

2.2. Adhere to all applicable international, federal, state, and local laws and regulations.

2.3. Adhere to the contractual and licensing agreements to which the College has entered related to use of third-party resources (e.g., software) and require each individual using the resource to comply.

2.4. Users must not utilize College Technology Resources to violate copyright, patent, trademark, or other intellectual property rights.

2.5. Users may not engage in unauthorized use of College Technology Resources, regardless of whether the resource used is securely protected against unauthorized use.

2.6. Use College Technology Resources and/or College Data only for the purpose for which access has been granted.

2.7. Unauthorized use by a User of another User's personal identity or access (login) credentials is prohibited.

2.8. Secure login credentials to prevent unauthorized access.

2.9. Be held accountable for all activities conducted under their Authentication.

2.10. Secure College Data appropriately and in a secure location when not idle.

2.11. Respect the rights and privacy of others.

2.12. Acknowledge the finite capabilities of College Technology Resources. Users should limit their use of College IT resources accordingly and must abide by any limits placed on the use of its IT resources or on the use of any specific IT resource.

2.13. College Technology Resources may not be used to fundraise, advertise, or solicit unless that use is approved in writing and in advance by the College.

2.14. College Technology Resources may not be used to engage in political activities.

2.15. College Technology Resources may not be used to operate a business or for commercial purposes unless that use is approved in advance by the College.

2.16. College Technology Resources may not be used to support the operations or activities of organizations that are not affiliated with the College unless that use is approved in advance by the College.

2.17. Viewing, downloading, uploading, or engaging in Pornography and Sexually Explicit Content is strictly prohibited.

2.18. Altering, moving, or removing software, system logs, configuration files, or other files from a College Technology Resource.

2.19. Intentionally, recklessly, or negligently causing damage by any means to College Technology Resources and/or College Data.

## III. Enforcement

3.1. Use of College Technology Resources is a privilege and not a right. A User's access to College Technology Resources may be limited, suspended, or terminated if that User violates this Policy. Alleged violations of this Policy will be addressed by the Chief Information Officer (CIO) or his/her designee.

3.2. Users who violate this Policy, other College policies, or external laws may also be subject to disciplinary action and/or other penalties. Disciplinary action for violation of this Policy is handled through the College's normal student and employee disciplinary procedures.

3.3. Any individual affiliated with the College who violates this Policy will be subject to appropriate corrective action, including, but not limited to, termination of the individual's relationship with the College.

3.4. In addition to its own administrative review of possible violations of this Policy and other College policies, the College may be obligated to report certain uses of College Technology Resources to law enforcement agencies.

3.5. If the CIO determines that a User has violated this Policy and limits, suspends, or terminates the User's access to any Mountwest IT resource as a result, the User may appeal that decision to the CIO.

3.6. The CIO may temporarily suspend or deny a User's access to College Technology Resources when he/she determines that such action is necessary to protect such resources, the College, or other Users from harm. In such cases, the CIO will promptly inform other College administrative offices, as appropriate, of that action. IT staff reserve the right to suspend or deny a User's access to the local resources they administer for the same reasons without the prior review and approval of the CIO, provided that they immediately notify the CIO of that action. A proper review of the case will take place upon notification to the CIO.

## IV. Security & Operations

4.1. The College may, without further notice to Users, take any action it deems necessary to protect the interests of the College and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may be taken at the institutional or local level, and may include, but are not limited to, scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and blockade of unauthorized access to, and unauthorized uses of, its networks, systems, and data. Local and central institutional IT resource administrators may take such actions in regard to the resources they manage without the prior review and approval of the CIO as long as the actions involve automated tools and not direct human inspection.

4.2. When the College receives a Freedom of Information Act request, subpoena, litigation, or other similar request for information or documents, it will take necessary measures to access College Technology Resources in order to obtain the requested College Data and comply with its legal obligations.

4.3. Authorized Individuals who use College Technology Resources are advised that they should have no expectation of privacy or confidentiality in connection with anything they create, store, send, or receive on College Technology Resources.

4.4. Monitoring and Routine System Maintenance:

4.4.1. While the College does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of those resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities. The College may access IT resources as necessary for system maintenance, including security measures.

4.4.2. In order to protect User privacy, the CIO or his/her designee must review and approve any request for access by a person to an individual User's personal communications or electronically stored information within College Technology Resources.

## VIII. Revisions

January 31, 2024

November 21, 2024