POLICY Board of Trustees - Montgomery College **66001**

Chapter: Fiscal and Administrative Affairs Modification No. 003

Subject: **Acceptable Use of Information Technology**

I. To provide adequate and continuing support of the instructional mission of the College, it is the intent of the Board of Trustees to provide a policy for acceptable use of information technology resources made available by the Board to students, faculty and staff, and any non-College individuals and entities specifically authorized to use these resources. The same acceptable standards for all users with regard to the use of facilities, equipment and tools, as well as acceptable standards of behavior toward individuals while using these resources, apply to the use of information technology resources as well. The ability to use these resources is a privilege, not a right or guarantee, based on Board of Trustees' priorities and available funding. No one can or should assume that because this policy is silent on a particular act or behavior, or that just because one is capable of doing something, that it is then acceptable, condoned, or legal.

II. The College, through policies, procedures, and regulations has already established acceptable uses of College resources. The College has also defined and established processes available to all students, faculty and staff regarding such issues as harassment, standards of behavior, plagiarism, conflict of interest and unethical conduct, as evidenced in the Board of Trustees' policies and the Montgomery College Student Handbook. There already exist federal, state, and local laws, rules and regulations regarding theft, copyright infringements and other unlawful acts. Those same disciplinary actions that apply to the misuse of other resources and behaviors may be applied to misuse of information technology resources. All users who request and/or are given access to College-owned and operated information technology resources agree to use those resources in a manner consistent with the mission of the College and in compliance with Board of Trustees' policies, as well as all applicable laws, procedures, rules and regulations.

III. The President is authorized to establish procedures to implement this policy.

_____

Board Approval: July 21, 1997(Interim Policy); February 19, 2001; April 28, 2014.

Chapter: Fiscal and Administrative Affairs Modification No. 004

Subject: **Acceptable Use of Information Technology**

I. Definitions

A. Electronic Communications – Electronic messaging systems, including, e-mail, is available for communications in a responsible manner, in accord with College policy. It is intended for communication between individuals and clearly identified groups of interested individuals, not for unauthorized mass broadcasting. Electronic communications will also include other College sanctioned methods for communicating to the College community.

B. Information Technology Resource ("IT Resources") – Any and all parts of the College's network, computer hardware, software, mobile computing or telephone devices, related peripheral support (i.e., printers, scanners, network, etc.), or telephone/communications system/resource, that is administered, allocated and managed by and for the College either on-site or at a College administered location or remotely. This includes devices not owned by the College but which are connected to the college network or any related peripheral devices.

C. Password – Passwords are unique alpha/numeric combinations provided only for the user's personal use. Passwords are not to be used by anyone else.

D. System Administrator/s – The person/s responsible for administering and managing hardware and software resources of the College network. This includes personnel in the Office of Information Technology ("OIT") as well as persons employed within other College units with similar responsibilities.

E. Telephone/Communications Systems/Resources – Telephone/communications systems/resources are hardware and software that enable transmission, including voice and video, over telephone/data lines.

F. Vice President of Instructional and Information Technology/Chief Information Officer ("VP/CIO") – The administrator charged with directing and managing efforts related to IT Resources under these procedures.

G. Website or Webpage – Any site created and maintained on College web servers, or in furtherance of College business, whether personal, by a unit or department, or as an official instrument of the College.

II. User Responsibilities

Users are expected to comply with legal, policy and procedure requirements and standards related to the use of IT Resources. These requirements include:

A. The User is expected to abide by College security requirements and will:

1. Use the College's IT Resources legally and in accordance with any required authorization.

2. Neither endanger the security of any College computer or network facility

nor willfully interfere with others' authorized computer use.

3. Connect to College networks, including wireless networks, only with equipment/computers, including desktops, laptops, tablets, and smartphones or any other equipment, that meet any applicable College OIT technical and security standards.

4. Provide reasonable security to one's passwords and respect the privacy and security of others' passwords.

5. Recognize that confidential information must be protected appropriately and in accordance with College policy. The College cannot guarantee the privacy of computer files, electronic communications, or other information stored on or transmitted by computer or other device.

B. The User is expected to:

1 Abide by law in not participating in computer theft, computer trespass, invasion of privacy, computer forgery, password disclosure, or misleading transmittal of names or trademarks.

2. Abide by the laws of copyright and/or license agreements.

3. Understand that the College will not defend the user against any charges of criminal acts outside of the scope of employment involving the use of College-owned IT Resources.

4. Use the College's IT Resources for College business and mission purposes and limit other uses to occasional occurrences; such other uses must not have undue impact on the operation of the College's IT Resources, adversely affect the work or mission of the College, whether performed by the user or others, or violate any other provisions of policy or practice standards of the College.

5. Take responsibility for the materials they transmit through the College's electronic communications system and other College provided IT Resources and not violate College policy with such transmission.

6. Not harass, threaten, or otherwise cause harm to specific individuals through electronic communication; and not create what a casual observer might reasonably perceive to be an atmosphere of harassment, including sexual harassment. A casual observer may be anyone such as a fellow student, employee, or visitor.

C. Users shall adhere to a standard of behavior that is not disruptive to the business of the College and will:

1. Not impede, interfere with, impair or otherwise cause harm to the activities of others;

2. Not download or post to College computers, or transport across College networks, material that is illegal, proprietary, subject to copyright protection, in violation of College contracts or third party intellectual

property rights, or that otherwise exposes the institution to liability.

3. Not use the College's electronic communication facilities to attempt unauthorized use, or interfere with others' legitimate use of any computer or network facility anywhere.

4. Share computing resources in accordance with policies set for computers involved.

5. Use caution in downloading or distributing information and shall not create, install, or knowingly distribute computer malware or other destructive program on any IT Resource, regardless of whether any demonstrable harm results.

6. Use available software and hardware "as is" without attempting to modify or reconfigure the software or hardware of any IT Resource.

7. Be cautious of receiving phishing e-mails, spam, and other types of electronic fraud, and not open or redistribute any suspicious items.

8. Use caution when sending out any electronic communication which is or that may appear to be an official communication on behalf of the College except when appropriate and authorized.

D. Users will be good stewards in the care and safeguarding of files and records and will:

1. Assure appropriate backup of data in their possession or control to prevent loss of College data; users may rely on backups announced by OIT but are encouraged to augment these backups as appropriate.

2. Recognize that these responsibilities extend beyond the confines of any employment or contractual relationship with the College, and that any attempt to destroy or alter College records for purposes other than routine maintenance, whether hard copy or electronic, will be subject to disciplinary/legal action.

3. Comply with periodic requests to alter/change passwords and any training requirements associated with continued use and access to the College's resources.

III. College Responsibilities

A. The College is expected to adhere to industry standards and other best practices with regard to computer and telephone systems to provide adequate access to these resources with the optimum service levels possible, in accordance with legal requirements, Board of Trustees' policy, and within the approved budget. The Vice President of Instructional and Information Technology/Chief Information Officer ("VP/CIO") is charged with directing and managing these efforts.

B. The College makes no warranties of any kind, either express or implied, that the functions or services provided by or through technology resources will be error free or without defect. The College will not be liable for any damage users may

suffer, including but not limited to loss of data, service interruptions or failure to deliver services. In addition, the College makes no representation or warranties, either express or implied, for data, information and materials obtained over the Internet and will not be liable for any damage users may suffer as a result of relying upon such data or information.

C. College System Administrators are expected to abide by College standard security requirements and will:

1. Maintain computing resources for a consistent user experience, with consideration to environmental conditions, access requirements of given individuals, security issues, safety issues, and budgetary resources.

2. Take all reasonable precautions to protect IT Resources.

3. Take reasonable steps to assure that confidential information is protected appropriately and in accordance with College policy, recognizing that the College cannot guarantee the privacy of computer data, electronic mail, or other information stored on or transmitted by computer.

D. College System Administrators will be good stewards in the care and safeguarding of files and records and will:

1. Provide access to IT Resources to the extent permitted by law, budgetary resources, technical capability, and adherence to established standards approved by the VP/CIO.

2. Complete system server back-ups as often as is necessary to safeguard files and records.

E. College System Administrators shall adhere to a standard of behavior that is not disruptive to the business of the College and will:

1. Reserve the right to block incoming mass mailings (“spam”) or malicious messages, and to block all Internet communications from sites that are involved in extensive spamming or other disruptive practices.

2. Respect privacy and refrain from access of computer files, electronic communication, or other information stored on or transmitted by College computing resources unless authorized as designated under these procedures.

3. Permit officially authorized College organizations to send appropriate announcements to all of their members by electronic communications and facilitate the College’s need to send electronic communications to large groups, including disseminating administrative notices, notifying students of educational opportunities, or otherwise carrying on the work of the College subject to reasonable approval or authorized procedures and limitations.

4. Treat all users fairly and equitably and not interfere with users’ electronic communication, especially in any way that would be interpreted as

favoring one side of a controversy or suppressing an unpopular opinion or topic.

F. College System Administrators are expected to abide by existing legal requirements and those that may be added from time to time and will:

1. Provide computers and networks to serve the College community in the furtherance of the College's mission, in accordance with College policies and procedures, federal, State of Maryland and local laws and regulations.

2. Report all cases of suspected misuse to the Information Technology Policy Administrator (ITPA).

G. College System Administrators will take all reasonable measures to insure adequate safety of College IT Resources and the data maintained thereon and will:

1. Provide opportunities for training to College users, and otherwise make every reasonable effort to inform users of College policies and procedures with regard to the use of IT Resources.

2. Develop and publish a schedule for users of required password changes, implementing such with as little interruption of services as is possible.

3. Apprise users of planned interruptions of service for maintenance and back-ups, when required.

4. Apprise users of unplanned, but necessary and required interruptions of service as soon as is practically possible.

5. Restore service to users as quickly as is practically possible.

H. College System Administrators are required to establish reasonable and fair processes and standards for user access to College IT Resources. It is considered an abuse of College policy to try to gain access to systems, files, or communications for which the user does not have authorized access. Access to IT Resources is based on the principle of least privilege to perform job responsibilities, ensuring minimal user access privileges on computers and to data, based on users' job necessities. This also applies to processes on the College's IT Resources; each system component or process should have the least authority necessary to perform its necessary functions.

I. System Administrators of academic laboratories may post additional standards, guidelines or practices that supplement these procedures.

IV. Privacy Issues of Computer Use and Communications

A. Users are reminded that all information created or received for work purposes and/or contained in College computing equipment files, servers or electronic communications are depositories and are public records that are created and maintained by public funds, and are available to the public unless an exception

under the Maryland Public Information Act applies. Thus, users should have no expectation of privacy. The College respects the desire for privacy and voluntarily chooses to refrain from routinely inspecting user files and electronic/telephonic communications. However, the College may monitor access to the equipment and networking structures and systems for such purposes as ensuring the security and operating performance of its systems and networks; reviewing employee performance; and enforcing College policies, procedures, standards, and applicable laws.

B. Examination, access, or the grant of access to current users' files, electronic communications, or network transmission contents by OIT staff or its contractors, other than for the limited purposes authorized in IV, C below, must be authorized beforehand by written approval from a Senior Vice President and the Office of the General Counsel.

C. Legitimate reasons exist for persons other than the user to access IT Resources without approval. OIT personnel and contractors may access IT Resources for the following purposes without the authorization required in IV, B above: 1) access to protect the operations and systems of the College or ensure integrity or continuation of operations, 2) to meet legal requirements, 3) the backup and caching of data and communications, 4) the logging of activity and the monitoring of general usage patterns, not concentrated on an individual user; 5) the scanning of systems and network ports for anomalies and vulnerabilities, 6) the repair of individual and network devices and other such activities that are necessary for the deployment, redeployment and maintenance of IT Resources for which OIT is responsible. This activity shall not involve data associated with individually identifiable persons except to the extent required for system operations.

V. College Web Servers/Electronic Publishing

The development and maintenance of a departmental, unit, or personal website or homepage is permitted through the College's computing resources. Electronic publishers are expected to observe all applicable laws, rules and regulations, are solely responsible for content and maintenance of these websites and for keeping such site free from any personally identifiable information regarding the College, its students, faculty, or staff, and will not in any way indicate or imply that such material is endorsed by the College. Personal homepages/sites shall contain a disclaimer stating "that the page/site is not endorsed, sponsored or provided by or on behalf of Montgomery College."

VI. Computer Hardware and Software

A. Warranty Agreements

1. It is the practice of the College to respect all manufacturer warranty agreements and to service College-owned computer hardware within manufacturer guidelines by authorized warranty service technicians.

2. It is the practice of the College to respect all computer software copyrights and to adhere to the terms of all software licenses to which Montgomery College is a party; users of software are required to comply with software licensing agreements.

B. Acquisitions and Provisioning of IT Resources

1. In an effort to maintain a cost effective, legally compliant, and secure technology environment at the College, the provisioning and disposal of IT Resources will be managed by OIT. OIT will provide collegewide coordination in the requisition process and manage the acquisition, configuration, deployment, and disposal process.

2. All servers storing College information or running College business or instructional applications must be housed in an OIT operations center, unless otherwise approved by the VP/CIO and properly secured and maintained according to OIT standards.

3. OIT will track all purchases, warranties, licenses and installations, and will perform or assist with installation of all College-owned hardware and software.

VII. Policy Assurance

The ITPA, in conjunction with the Office of the General Counsel, is charged with ensuring compliance with policies and procedures applicable to information technology.

A. The ITPA is responsible to investigate on behalf of the Office of General Counsel (OGC) all reported violations and keep a record for OGC of each one. In the case of an alleged intellectual property infringement notification, the ITPA will respond in writing to the party sending the notification after conducting an investigation, maintaining a copy in ITPA files, subject to other instructions from the OGC.

B. The ITPA's investigation in coordination with OGC will include gathering information, determining the likelihood that a violation has occurred, notifying all appropriate parties affected, and addressing IT system damage and repair actions. The ITPA will assess each situation and involve other College staff and/or external agencies as necessary to protect and repair the IT Resources of the College.

C. The ITPA will adhere to College policies and procedures in the investigation and disposition of each incident. Investigations may include such activities as:

1. A written notice to the supervisor of a person alleged to have committed a violation, with a request for appropriate actions;

2. A written notice to the Vice President of Human Resources, Development, and Engagement, requesting appropriate actions;

3. A written notice to the General Counsel requesting directions and guidance, including instances in which the ITPA recommends the involvement of law enforcement agencies or any other entity that may have jurisdiction.

D. The ITPA will submit a report to the President of the College or designee with a summary of incidents related to violation of the Acceptable Use Policy from time to time, but no less often than annually.

E. The ITPA has the authority to remove or restore access to IT Resources to any user who is believed to have violated the Acceptable Use Policy and/or procedures of the Acceptable Use Policy. Written notice must be given the user, the user's supervisor, and the General Counsel when this action is anticipated. No further sanctions are within the ITPA's authority.

F. Appeals concerning the decision and actions of the ITPA are permitted. The appeals process is:

1. All appeals must be addressed to the VP/CIO, within ten (10) days of the decision of the ITPA.

2. Appeals must be in writing, stating specifically the basis of the appeal.

3. The VP/CIO will make a decision regarding the appeal within ten (10) days of receipt of the appeal.

4. The decision of the VP/CIO regarding an appeal will be in writing.

5. Nothing in this process prevents the user whose access to IT Resources has been restricted from pursuing other avenues of appeal that may be available under College policy or law.

_____

Administrative Approval: February 19, 2001; August 27, 2001; March 25, 2004; April 28, 2014.