MOUNTWEST COMMUNITY & TECHNICAL COLLEGE

BOARD OF GOVERNORS

Policy No. I - 2

INFORMATION SECURITY

1 General Information:

1.1. Scope: This policy applies to all College employees (faculty, staff, student, contract employee, or contract partner) who have access to College information and to systems that store, access, or process the information.

The College's information resources are vital academic and administrative assets which this policy establishes guidelines and responsibilities for information security and the protection of college information requires appropriate safeguards. Paper-based systems, computer systems, networks, and data are vulnerable to a variety of threats. These threats have the potential to compromise the integrity, availability, and confidentiality of the information. Effective security management programs must be employed to appropriately eliminate or mitigate the risks posed by potential threats to the College's information resources. Measures shall be taken to protect these resources against unauthorized access, disclosure, modification or destruction whether accidental or deliberate.

1.2 Authority: W. Va. Code §18B-1-6

1.3 Passage Date: November 22, 2021

1.4 Effective Date: December 22, 2021

2 Policy: (Refer to Section 5 for definitions of specific terms)

2.1 Principles

2.1.1. Responsibility for controlling access and the development and implementation of appropriate security policies, standards, guidelines, practices, and educational programs rests with the information owners or their designees who are responsible for collecting and maintaining information as well as those charged with operating the College's information technology environments (includes all central and decentralized IT providers / Information custodians). The College is committed to the principle of appropriate access. For all information, owners and custodians should make informed decisions regarding the appropriate access that will be provided. Stewardship of the information may depend on its nature and be governed by federal laws, state laws, requirements of external regulatory organizations, and/or College policy.

2.2. Administration

2.2.1. An ISO (Information Security Officer) role must be assigned. This individual must perform, contract, or delegate the necessary functions and responsibilities of the position. (GOT ISG - sections 3.2 and 4.1)

2.2.2. All information resources, regardless of medium, will be used, maintained, disclosed, and disposed of according to law, regulation, or policy. (GOT ISG - section 7.3)

2.2.3. All employees and others who access computer systems will be provided with sufficient training in policies and procedures, including security requirements, correct use of information resources, and other organizational controls. (GOT ISG - sections 4.1 and 11.0)

2.2.4. A documented risk analysis program will be implemented and a risk analysis will be conducted periodically. (GOT ISG - sections 4.1 and 6.0)

2.2.5. A cost effective incident response/business recovery plan will be maintained providing for prompt and effective continuation of critical missions in the event of a security incident. (GOT ISG - sections 4.1 and 9.0)

2.2.6. Procedures, guidelines, and mechanisms that are utilized during a security incident, along with the roles and responsibilities of the incident management teams, must be established and reviewed regularly.

2.3. Access Controls (GOT ISG - sections 4.2 and 5.0 -5.5)

2.3.1. Access controls must be consistent with all state, federal, and local laws and statutes and will be implemented in accordance with this policy.

2.3.2. Procedures must be implemented to protect information resources from accidental, inadvertent, unauthorized, or malicious disclosure, modification, or destruction.

2.3.3. Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.

2.3.4. Individual users must have unique userids and passwords.

2.3.5. All employees must be accountable for their computer and userids and for any actions that can be identified to have originated from these accounts.

2.3.6. When employees are transferred or their employment is terminated, access, userids and authorizations will be immediately modified or terminated as required.

2.3.7. Confidential or sensitive data (i.e., credit card numbers, calling card numbers, log on passwords, etc.) must be encrypted before being transmitted through the Internet.

2.3.8. The network access firewall and/or secure gateway must be configured to deny all incoming services unless explicitly permitted.

2.3.9. Data and supporting software necessary for the continuation of university functions will be backed up periodically at a frequency determined by risk analysis.

2.3.10. All information assets must be accounted for and will have an assigned owner. (GOT ISG - section 7.0) Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.

2.3.11. All access to computing resources will be granted on a need-to-use basis.

2.3.12. The owner and custodian of information will determine its classification based on the circumstances and the nature of the information.

2.3.13. The owner and custodian will determine the protective guidelines that apply for each class of information. They include the following:

2.3.14. Access

2.3.15. Distribution within the university

2.3.16. Distribution outside the university

2.3.17. Electronic distribution

2.3.18. Disposal/Destruction

2.3.19.   All programmable computing devices must be equipped with up-to-date virus protection software.

2.3.20.   Virus protection procedures will be developed to address system protection.

2.4. Personnel Practices (GOT ISG - sections 4.3 and 10.0 -10.8)

2.4.1. All IT assets, including hardware, software, and any physical or virtual network that pass through these assets are owned by Mountwest Community & Technical College unless excepted by contractual agreement.

2.4.2. Information resources are designated for authorized purposes only. The college reserves the right to monitor and review employee use as required for legal, audit, or legitimate authorized State operational or management purposes.

2.4.3. All employees must receive an appropriate (as determine by the information owner and information security officer) background check.

2.4.4.   All employees must sign a confidentiality statement indicating that they have read,understand, and will abide by college policies and procedures regarding IT security.

2.4.5. All vendors and contractors must sign and abide by a contract/confidentiality statement to ensure compliance with state and university information security policies and procedures. (GOT ISG - section 8.0)

2.4.6. All employees must abide by rules regarding acceptable and unacceptable uses of IT resources (please refer to the current Mountwest Community & Technical College Information Technology Environment Acceptable Use Policy.

2.5. Physical and Environmental Security (GOT ISG - sections 4.4 and 12.0 -12.6)

2.5.1. Information resource facilities will be physically secured by measures appropriate to their critical importance.

2.5.2. Security vulnerabilities will be determined and controls will be established to detect and respond to threats to facilities and physical resources.

2.5.3. Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.

2.5.4. Equipment will be secured and protected from physical and environmental damage.

2.5.5. Equipment used outside State premises should be given the same degree of security protection as that of on-site information resource equipment.

3 Enforcement

3.1. Enforcement of this policy is the responsibility of the Chief Information Officer or their designate.

3.2. Any employee found to have violated this policy will be subject to disciplinary or corrective actions based upon the policies, rules, and procedures of the relevant group to which the employee belongs, and may include sanctions including, but not limited to, revocation of employee or student privileges up to and including expulsion or termination of employment or contract. Certain violations, misuse, or disclosures of confidential information may include civil and/or criminal penalties.

4 Responsibilities

4.1.   The Chief Information Officer is responsible for administering the provisions of this policy and the State of West Virginia Information Security Guidelines.

4.2.   The director of a department shall be responsible for ensuring that an appropriate security program is in effect and that compliance with this policy and State of West Virginia Information Security Guidelines is maintained for information systems owned and operationally supported by the department.

4.3.   The director of a department which provides operational support (information custodian) for information systems owned by another Mountwest Community & Technical College department (information owner) shall have joint responsibility for ensuring that an appropriate security program is in effect and that compliance with State of West Virginia Information Security Guidelines is maintained for the supported information systems.

4.4.   Information maintained on an individual workstation or personal computer must be afforded the appropriate safeguards stated in this policy and the State of West Virginia Information Security Guidelines. It is the joint responsibility of the department director and operator/owner of that workstation or personal computer to insure that adequate security measures are in place, i.e., the concepts of information owner/custodian responsibilities extend throughout the organization.

4.5.   Operational responsibility for compliance with this policy and State of West Virginia Information Security Guidelines may be delegated by the department head or director to the appropriate information system support personnel (e.g. System Administrators) within the department.

5 Definitions

5.1. Access - to approach or use an information resource.

5.1.1. Unauthorized Access -

5.1.1.1.   Access to employee, student, patient, donor, or patron information not necessary to carry out your job responsibilities.

5.1.1.2.   Access to the records of a student, employee, patient, donor, or patron for which you are not legally responsible or for which you do not have signed authorization. This includes spouse, parents, and other relatives not under your guardianship.

5.1.1.3.   Release of employee, student, patient, or donor information to unauthorized internal users.

5.1.1.4.   Release of more employee, student, patient, donor, or patron information to an authorized individual than is essential to meeting the stated purpose of an approved request.

5.1.1.5.   Release of information to any external agency unless you are designated as the owner of the information requested.

5.1.1.6.   Release of information protected by College, State, and Federal guidelines, policies, regulations, statutes, and procedures pertaining to confidentiality and privacy, including, but not limited to, the Family Educational Rights and Privacy Act of 1974 (FERPA), and WV Code §18-2-5f.

5.2. Access Control - the enforcement of specified authorization rules based on positive identification of users and the systems or data they are permitted to access.

5.3. Authentication - the process of verifying the identity of a user.

6.4. Chief Information Officer - the person responsible for the college's information resources

5.5. Confidentiality Agreement -

5.5.1. I acknowledge the confidential nature of non-public information held by me regarding our employees, students, patients, donors, patrons, and other members of the Mountwest community. Consistent with applicable policies and guidelines, I will respect and safeguard the privacy of members of the Mountwest community and the confidential nature of their information. Without limiting the general nature of this commitment, I will not access or seek to gain access to confidential information regarding any past or present employee, student, patient, or donor of Mountwest Community & Technical College except when fulfilling my job responsibilities. I understand that in this context, confidential information is defined as all non-public information that can be personally associated with an individual.

If in the course of executing my job responsibilities, I accidentally access information that others might consider inappropriate for me to access, I will not disseminate any such information without proper authorization.

I will not use another's computer sign-on or computer access code or provide another the use of an individual's sign-on code to gain access to confidential information without proper authorization. I will not disclose confidential information to those who are not authorized to receive it. In addition, I will not, without proper authorization, copy or preserve confidential information by manual, electronic, or any other means, nor will I disseminate any such information without proper authorization. If I am in doubt about whether the authorization provided is "proper", I will consult the defined Information Owner for guidance (see http://www.mctc.edu)

I acknowledge that should I receive Account Names (userids) and Passwords that the passwords are the equivalent of my signature. I understand that I will only access information that is required for me to perform my assigned tasks. I acknowledge that if I disclose passwords to any other person, I will be fully accountable and responsible for any use or misuse by that individual to the same extent as if I had performed the act or omission. If I have any reason to believe that the confidentiality of my passwords has been violated, I will notify my department head or supervisor immediately and ensure that the passwords are promptly changed. IfI believe I have been asked to access or release information that lies outside my defined job responsibilities, I will notify the College Information Security Officer and request guidance.

I understand that if I move to another department on campus, I will retain the same account name and password, although my security access may change. I understand that if my relationship with the College is terminated for any reason, I will no longer have access to College equipment and data.

I understand and agree that a violation of any portion of the confidentiality policy renders me subject to disciplinary or corrective actions that may result in sanctions including, but not limited to revocation of employee or student privileges up to and including expulsion, or termination of employment or contract. Under certain

circumstances, disclosure of confidential information may include civil and/or criminal penalties.

_____   _____

SIGNATURE   DATE

_____

PRINT FULL NAME

5.6. Employee - Individuals employed on a temporary or permanent basis by Mountwest Community & Technical College or its associated organizations; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the university to be subject to this policy.

5.7. Encryption - process of encoding electronic data that makes it unintelligible to anyone except the intended recipient.

5.8. Firewall - specialized computers and programs, residing in a virtual area between an organization's network and outside networks, which are designed to check the origin and type of incoming data in order to control access, and block suspicious behavior or high-risk activity.

5.9. Information Assets - Any of the data, hardware, software, network, documentation, and personnel used to manage and process information.

5.10. Information Classification (or class) - An assessment of the importance of the information resource. This classification may have multiple dimensions. On the Privacy dimension: Confidential, Private, and Public. On the Value dimension: Mission Critical, Essential, and Desirable.

5.11. Information Custodian - the person or unit assigned to supply services associated with the data e.g., database administration, systems administration.

5.12. Information Owner - the person(s) ultimately responsible for an application and its data viability. In those cases where an information owner is not specifically defined the CIO is the default owner.

5.13. Information User - a person authorized to access an information resource.

5.14. Information Security - those measures, procedures, and controls that provide an acceptable degree of safety for information resources, protecting them from accidental or intentional disclosure, modification, or destruction.

5.15. Information Security Officer (ISO) - the person designated by the university head to administer the university's information security program. The ISO is the university's internal and external point of contact for all information security matters.

5.16. Password - a string of characters known to a computer system or network and to a user who must enter the password in order to gain access to an information resource.

5.17. Risk Analysis - the evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

5.18. Security Incident - an event that results in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.

5.19. Threat - includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.