EASTERN WEST VIRGINIA COMMUNITY & TECHNICAL COLLEGE
BOARD OF GOVERNORS
POLICY NO. BP-6.13

TITLE: SECURITY OF INFORMATION TECHNOLOGY

SECTION 1. GENERAL

1.1. This policy establishes guidelines and responsibilities for Eastern West Virginia Community and Technical College employees regarding information security and the protection of agency information resources. This information is based on the State of West Virginia Information Security Guidelines issued by the Governor's Office of Technology.

1.2. Authority - State of West Virginia Security Guidelines

1.3. Effective Date - **March 16, 2016**

SECTION 2. SCOPE AND APPLICABILITY

2.1. This policy applies to all Eastern West Virginia Community and Technical College employees who have access to agency information and to systems that store, access, or process the information.

SECTION 3. STATEMENT

3.1. It is the policy of Eastern WV Community and Technical College to allow access to computing resources by all college faculty, staff, and students. Access may also be granted to individuals outside the college for purposes consistent with the mission of the college.

3.2. Administration

3.2.1 An ISO (Information Security Officer) role must be assigned. This individual must perform, contract, or delegate the necessary functions and responsibilities of the position.

3.2.2 All information resources, regardless of medium, will be used, maintained, disclosed, and disposed of according to law, regulation, or policy.

3.2.3 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.

3.2.4 A documented risk analysis program will be implemented and a risk analysis will be conducted periodically.

3.2.5 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. 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.

3.3 Access Controls

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

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

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

3.3.4 Individual users must have unique user ids and passwords.

3.3.5 All employees must be accountable for their computer, account, and password and for any actions that can be identified to have originated from them.

3.3.5.1 When employees are transferred or their employment is terminated, user ids and authorizations will be disabled immediately.

3.3.6 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.

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

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

3.3.9 All information assets must be accounted for and will have an assigned owner. Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented. All access to computing resources will be granted on a need-to-use basis.

3.3.10 Human Resources will be responsible for notifying Technology Services of termination dates for exiting employees.

3.3.11 The owner or custodian will determine the protective guidelines that apply for each level of information. They include the following: Access, distribution within the college, electronic distribution, and disposal/destruction.

3.3.12 Technology Services will insure that all programmable computing devices are equipped with up-to-date virus protection software~~;~~. Virus protections procedures will be developed to address system protection.

3.4 Personnel Practices

3.4.1 All IT assets, including hardware, software, and data are owned by Eastern WV Community and Technical College unless excerpted by contractual agreement.

3.4.2 Information resources are designated for authorized purposes only. Eastern WV Community and Technical College reserves the right to monitor and review employee use as required for legal, audit, or legitimate authorized State operational or management purposes.

3.4.3 The Human Resource Administrator must assure that all employees receive an appropriate background check (where applicable) consistent with legislative rule and the Institutional policy.

3.4.4 All employees must sign a confidentiality statement indicating that they have read, understand and will abide by agency policies and procedures.

3.4.5 All vendors and contractors must sign and abide by a contract/confidentiality statement to ensure compliance with state and agency information security policies and procedures.

3.4.6 All employees must abide by rules regarding acceptable and unacceptable uses of IT resources.

3.5 Physical and Environmental Security

3.5.1 Information resource facilities will be physically secure by measures appropriate to their critical importance.

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

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

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

3.5.5 Equipment used outside the college premises will be given the same degree of security protection as that of the on-site information resource.

SECTION 4. DEFINITIONS

4.1. Access - To approach or use an information resource.

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

4.3. Authentication – The process of verifying the identity of a user.

4.4. Chief Information Officer – The person responsible for the agency's information resources.

4.5. Custodian of Information – The person or unit assigned to supply services associated with the data.

4.6. Employee – Individuals employed on a temporary or regular basis by Eastern West Virginia Community and Technical College; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the institution to be subject to this policy.

4.7. Encryption – Process of encoding electronic data that makes it unintelligible to anyone except the intended recipient.

4.8. Firewall – Specialized computer 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.

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

4.10. 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.

4.11. Information Security Officer (ISO) – The person designated by the Chief Information Officer to administer the agency's internal and external point of contact for all information security matters.

4.12. Owner of Information – The person(s)/department ultimately responsible for an application and its data viability.

4.13. 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.

4.14. Risk Analysis – The evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.

4.15. Security Incident – An event that results in unauthorized access, loss, disclosure, modification, or destruction or information resources, whether deliberate or accidental.

4.16. Threat – Includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.

4.17. User of Information – A person authorized to access an information resource.

SECTION 5. RESPONSIBILITIES AND PROCEDURES

5.1. Responsibilities

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

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

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

5.1.4 Mission Critical or Confidential 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 manager of the department/unit and operator/owner of that workstation or personal computer to insure that adequate security measures are in place.

5.1.5 Operational responsibility for compliance with this policy and the State of West Virginia Information Security Guidelines may be delegated by the Chief Information Officer to the appropriate technology services support personnel.

5.2 Procedures

5.2.1 When security and/or confidentiality of data files is breached by an employee, the matter shall be referred to the employee's department head for correction and discipline. The matter must be resolved in a manner acceptable to the Chief Information Officer and to the department head whose files have been improperly accessed or violated.

5.2.2 An employee who violates the security system by accessing confidential data without authorization will be subject to disciplinary action. Violation of the security system by an employee includes but is not limited to the following:

5.2.2.1 Obtaining a password(s) without proper authorization.

5.2.2.2 Helping an unauthorized person access confidential data or other information stored on the computer.

5.2.2.3 Allowing someone else to use their password to gain access to computerized information.

5.2.2.4 Sharing information from the data base with unauthorized personnel.

5.2.2.5 A student is considered to have breached the security system at any time he/she accesses any information contained on the administrative, financial, and/or student information system. A student's computer account, password and privileges may be suspended immediately. All violations will treated similar to that prescribed in the policy regarding academic cheating when the violation occurs within the scope of a class or a class exercise.

5.3 Enforcement

5.3.1 Enforcement of this policy is the responsibility of the Chief Technology Officer or their designee.

5.3.2 Any employee or student found to have violated this policy will be subject to disciplinary or corrective actions based upon college policies, Student Rights and Responsibilities rules, and procedures of the relevant group to which the individual belongs, and may include sanctions including, but not limited to, revocation of employee or student privileges up to and including termination of employment or suspension from school. Also disclosures of confidential information may include civil and/or criminal penalties.

BOARD OF GOVERNORS, CHAIR

5/12/16
DATE

APPROVED BY BOG: 3/16/16
APPROVED BY CABINET: 3/8/16
APPROVED BY IET: 02/26/2016