

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

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

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

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,

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 Resources Administrator must ensure that all employees receive an

appropriate background check (where applicable) consistent with legislative rule and the

- 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.

8. Firewall – Specialized computer and programs residing in a virtual area between an

SECTION 5. RESPONSIBILITIES AND PROCEDURES

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.

UN

WJ

WWW.WASHINGTONUNIVERSITYINST.EDU

CONFIDENTIAL

Confidential information may include penalties

[Handwritten signature]

BOARD OF GOVERNORS, CHAIR

DATE

11 18

CONFIDENTIAL

CONFIDENTIAL