

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 1 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

## 1.0 PURPOSE

This policy establishes guidelines and responsibilities for Blue Ridge 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.

## 2.0 SCOPE

This policy applies to all Blue Ridge Community and Technical College employees who have access to agency information and to systems that store, access, or process the information.

## 3.0 POLICY

### 3.1 Administration

- 3.1.1 The Director of IT Services will function as the ISO (Information Security Officer). This individual will perform, contract, or delegate the necessary functions and responsibilities of the position. (GOT ISG - sections 3.2 and 4.1)
- 3.1.2 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)
- 3.1.3 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)
- 3.1.4 A documented risk analysis program will be implemented and a risk analysis will be conducted periodically. (GOT ISG - sections 4.1 and 6.0)
- 3.1.5 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)
  - 3.1.5.1 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

### 3.2 Access Controls (GOT ISG - sections 4.2 and 5.0 -5.5)

- 3.2.1 Access controls must be consistent with all state, federal, and local laws and statutes and will be implemented in accordance with this policy.
- 3.2.2 Procedures must be implemented to protect information resources from accidental, inadvertent, unauthorized, or malicious disclosure, modification, or destruction.
- 3.2.3 Appropriate controls must be established and maintained to protect the confidentiality of passwords used for authentication.

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 2 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

- 3.2.4 Individual users must have unique userids and passwords.
- 3.2.5 All employees must be accountable for their computer and for any actions that can be identified to have originated from it.
- 3.2.6 When employees are transferred or their employment is terminated, userids and authorizations will be disabled immediately.
- 3.2.7 Confidential or sensitive data (i.e., credit card numbers, calling card numbers, log on passwords, etc.) must be encrypted before being transmitted on the Campus network or through the Internet.
- 3.2.8 The network access firewall and/or secure gateway must be configured to deny all incoming services unless explicitly permitted.
- 3.2.9 Data and supporting software necessary for the continuation of agency functions will be periodically backed up at a frequency determined by risk analysis.
- 3.2.10 All information assets must be accounted for and will have an assigned owner. **See: Blue Ridge Community and Technical College Data Policy (GOT ISG - section 7.0)**
  - 3.2.10.1 Owners, custodians, and users of information resources must be identified and their responsibilities defined and documented.
  - 3.2.10.2 All access to computing resources will be granted on a need-to-use basis.
- 3.2.11 Each owner or custodian of information will determine its classification based on the circumstances and the nature of the information.
- 3.2.12 The owner or custodian will determine the protective guidelines that apply for each level of information. They include the following:-  
Access - Distribution within Blue Ridge Community and Technical College - Distribution outside Blue Ridge Community and Technical College - Electronic distribution Disposal/Destruction. All guidelines must be consistent with FERPA.
- 3.2.13 All programmable computing devices must be equipped with up-to-date virus protection software, if available.
  - 3.2.13.1 Virus protection is available from IT Services for all campus managed computers.
  - 3.2.13.2 Virus programs and definitions are managed for Windows-based computers, via the AntiVirus server operated by IT Services. Non-windows computers are updated directly from virus-protection vendor.
  - 3.2.13.3 Users of non-networked equipment must consult with IT Services to determine best protection method.
  - 3.2.13.4 IT Services reserves the right to remove any non-compliant equipment from service.
- 3.3 Personnel Practices (GOT ISG - sections 4.3 and 10.0 -10.8)
  - 3.3.1 All IT assets, including hardware, software, and data are owned by Blue Ridge Community and Technical College unless excepted by contractual agreement.

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 3 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

- 3.3.2 Information resources are designated for authorized purposes only. Blue Ridge 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.
- 3.3.3 All employees must receive an appropriate background check.
- 3.3.4 All employees must sign a confidentiality statement indicating that they have read, understand, and will abide by agency policies and procedures regarding IT security.
- 3.3.5 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. (GOT ISG - section 8.0)
- 3.3.6 All employees must abide by rules regarding acceptable and unacceptable uses of IT resources. **See: Blue Ridge Community and Technical College Acceptable Use Policy**
- 3.4 Physical and Environmental Security (GOT ISG - sections 4.4 and 12.0 - 12.6)
  - 3.4.1 Information resource facilities will be physically secured by measures appropriate to their critical importance.
  - 3.4.2 Security vulnerabilities will be determined and controls will be established to detect and respond to threats to facilities and physical resources.
  - 3.4.3 Critical or sensitive data handled outside of secure areas will receive the level of protection necessary to ensure integrity and confidentiality.
  - 3.4.4 Equipment will be secured and protected from physical and environmental damage.
  - 3.4.5 Equipment used outside State premises will be given the same degree of security protection as that of on-site information resource equipment.

#### 4.0 ENFORCEMENT

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

#### 5.0 DEFINITIONS

- 5.1 Access - to approach or use an information resource.
- 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.
- 5.4 Chief Information Officer - the person responsible for the agency's information resources.
- 5.5 Custodian of Information - the person or unit assigned to supply services associated with the data.

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 4 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

- 5.6 Employee - Individuals employed on a temporary or permanent basis by the Blue Ridge Community and Technical College; as well as contractors, contractor's employees, volunteers, and individuals who are determined by the Bureau or Office 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 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.
- 5.11 Information Security Officer (ISO) - the person designated by the agency head to administer the agency's information security program. The ISO is the agency's internal and external point of contact for all information security matters.
- 5.12 Owner of Information - the person(s) ultimately responsible for an application and its data viability.
- 5.13 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.
- 5.14 Risk Analysis - the evaluation of system assets and their vulnerabilities to threats in order to identify what safeguards are needed.
- 5.15 Security Incident - an event that results in unauthorized access, loss, disclosure, modification, or destruction of information resources, whether deliberate or accidental.
- 5.16 Threat - includes any person, condition or circumstance that endangers the security of information, or information systems, in the context of Information Security.
- 5.17 User of Information - a person authorized to access an information resource.

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 5 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

I, \_\_\_\_\_, acknowledge I have received, read, and understand the Blue Ridge Community and Technical College IT Security Policy.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Name

<b>DOCUMENT:</b> IT Security Policy	<b>DOCUMENT NUMBER:</b>	<b>REVISION:</b> Original	Page 6 of 6
<b>SUBJECT:</b> Blue Ridge Community and Technical College IT Security		<b>EFFECTIVE DATE:</b> 07/01/2006	

I, \_\_\_\_\_, acknowledge I have received, read, and understand the Blue Ridge Community and Technical College IT Security Policy.

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Print Name