EASTERN WEST VIRGINIA COMMUNITY AND TECHNICAL COLLEGE
REGULATION NO. –AR-6.8

TITLE: **REMOTE ACCESS REGULATION**

DEFINITION: The purpose of this policy is to define requirements for connecting to the college's network. These requirements are designed to minimize the potential exposure to Eastern from damages which may result from unauthorized use of Eastern's resources. Damages include the loss of sensitive or confidential information, damage to public image and damage to critical internal systems.

EFFECTIVE DATE: March 8, 2016

SCOPE: This policy applies to all employees, contractors, vendors, and agents with a college-owned or personally-owned computer used to connect to the college's network. This policy applies to remote access connections used to perform work on behalf of Eastern including reading or sending email and viewing intranet web resources. Remote access implementations that are covered by this policy include, but are not limited to college owned data circuits, VPN, and WiFi.

REGULATION STATEMENT:

1. Storage of confidential information on any non-state owned device is prohibited. Confidential information may not be stored on any state owned portable device without prior written approval from the Chief Information Officer (or delegated authority). Approved storage on any portable device must be encrypted.

2. It is the responsibility of all employees and contractors with remote access privileges to Eastern's network to ensure that their remote access connection is given the same consideration as the user's on-site connection to Eastern.

3. All remote access users are expected to comply with all Eastern policies, may not perform illegal activities, and may not use the access for outside business interests.

REQUIREMENTS:

1. Remote access must be strictly controlled by the use of unique user credentials. For information on creating a strong password please review the college's Password Policy & Guidelines.

2. Remote access passwords are to be used only by the individual to whom they were assigned and may not to be shared.

3. All remote access connections that utilize a shared infrastructure, such as the Internet, must utilize some form of encryption. These include VPN, SSH and SSL, to name a few.

4. All hosts that are connected to the college's internal networks via remote access technologies must have up-to-date anti-virus software implemented.

5. All hosts that are connected to the college's internal networks via remote access technologies must have current operating system security patches installed.

Approved by LOT: 2/18/16
Approved by Cabinet: 3/8/16

6. Personal equipment that is used to connect to the college's networks must meet the requirements of college-owned equipment for remote access.

7. Organizations or individuals who wish to implement non-standard Remote Access solutions to the college's production network must obtain prior approval from the Chief Information Officer.

ENFORCEMENT: Any employee found to have violated this regulation may be subject to disciplinary action, up to and including termination of employment. Deliberate, unauthorized disclosure of confidential information may result in civil and/or criminal penalties.

DR. CHARLES TERRELL, PRESIDENT

3/29/16
DATE

Approved by LOT: 2/18/16
Approved by Cabinet: 3/8/16