EASTERN WEST VIRGINIA COMMUNITY AND TECHNICAL COLLEGE
REGULATION NO. – 6.11

TITLE: **MOBILE DEVICE**

DEFINITION: Eastern West Virginia Community and Technical College is committed to and encourages an open and collaborative environment through the use of mobile devices to facilitate academic interaction among students, faculty and staff. There is an inherent risk in utilizing mobile devices for this purpose, however, due to the ease with which these items can become lost or stolen.

The purpose of this regulation is to clearly state the college policy and user requirements necessary to mitigate this risk and to protect college or personal sensitive information stored on mobile devices.

EFFECTIVE DATE: March 22, 2017

POLICY:

It is the responsibility of anyone who utilizes the college's internal network for the purpose of accessing or processing college Sensitive Information using a Mobile Device to take appropriate measures at all times to safeguard that information. All such individuals ("Users") will ensure they are taking every reasonable precaution against accidental or intentional data compromise by implementing the measures prescribed in Appendix A of this policy for their Mobile Devices. Refer to Appendix B for added voluntary measures and helpful advice.

APPENDIX A: Standards

- No Mobile Device shall be used to store Sensitive Information unless the user complies with Security of Information Technology Policy.
- All use of Mobile Devices, college or personally owned, which utilize college network resources, will be subject to the provisions of the college's Acceptable Use Policy.
- If possible, all devices will be updated to the latest device operating system with the latest Security Patches.
- All applications (apps) will be updated with the latest Security Patches.
- All devices will be configured with a PIN, pattern, or password-enabled lock screen configured to activate at no more than 5 minutes of inactivity.
- All devices with built in Encryption capability will have onboard Encryption enabled.
- All devices will have Remote Wipe enabled either through Mobile Sync, a third party app or the manufacturer's website.
- All devices that have been used to store, access and/or process Sensitive Information will be wiped to remove such data before they are transferred to someone else through sale or gifting.
- In the event that a device which has been used to store, access and/or process Sensitive Information becomes lost, stolen or compromised, the owner must report it immediately to the Incident Response Team. Refer to the Incident Response Policy for the membership of this team and other information. Additionally, the user must immediately contact the Technology Services Department to request Remote Wiping through Mobile Sync if that service is utilized on the device. Otherwise, the user will request Mobile Wiping through the device's manufacturer.
- All college owned Android Mobile Devices will install the Google Device Policy app.

APPENDIX B: Guidelines

- Users should make sure they know the location of their Mobile Devices at all times. Mobile Devices should not be left unattended.
- Users should set up their device to back up their data at regular intervals. This will increase the user's confidence to use the Remote Wipe feature if they ever suspect their device to be lost or stolen. Be mindful, however, that any system chosen as the backup will now contain the College's Sensitive Information and the user will need to take appropriate measures to safeguard the data at that location. Users should consider using a password instead of a PIN or pattern for the device lock screen. Passwords, especially Strong Passwords, are much more secure.

- If possible, users should configure their devices to automatically wipe data after a preset number of unsuccessful password attempts.
- Users should not allow someone who is not authorized access to the college network to use their devices if they are used to process Sensitive Information.
- Users should install and regularly update Anti-virus Software.
- Users should learn how their Mobile Devices function. Not all users are aware that when they open an attachment from email most devices will store a copy of this attachment somewhere on the device. Users should consult the device user manual and other sources to learn how the device handles data.
- It is good practice to use a Mobile Device only for transitory storage of Sensitive Information. Users should delete any Sensitive Information stored on their devices immediately after the work with it is completed.
- Although not specifically required, it is good practice for personally owned Android users to accept and install the Google Device Policy App. Installing the app will provide key features such as syncing of contacts and calendar information. Users may choose to receive their email via Google's imap functionality; however, they will not have the ability to synch other Google managed data.

DEFINITIONS:

Mobile Device:	Any handheld or portable computing device including running an operating system optimized or designed for mobile computing, such as Android, Blackberry OS (RIM), Apple's iOS, or Windows Mobile. Any device running a full desktop version operating system is not included in this definition.
PDA:	A handheld device that combines computing, telephone/fax, internet and networking features.
Sensitive Information:	Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on the college interests, the conduct of college programs or the privacy to which individuals are entitled. Examples of such data would include the data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the college as requiring protective measures.
PIN:	Personal Identification Number: This can be any combination of numbers (usually a minimum of four) that is used to unlock a device.
Encryption:	The use of software or hardware to make data unreadable unless the device is presented with the correct password or PIN. Most Mobile Devices include this feature but require the user to enable it.
Remote Wipe:	The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.
Virus:	A computer program that is usually hidden within another seemingly innocuous program that has the function of stealing or destroying data or causing any number of unwanted system behaviors.
Malicious Software:	Often called malware, this is software designed to disrupt computer operation, gather Sensitive Information, or gain unauthorized access to computer systems.
Anti-virus Software:	Software designed to detect and/or remove Malicious Software and Viruses from a computer system.
Data Security Steward:	Individuals within the different college units, appointed by the college unit head, who are points of contact for unit data and for security violations or issues and act as a general reference for Information Security topics.

Strong Password: A password that is at least 8 characters long and is a combination of upper and lower case letters, numbers and characters. Strong Passwords do not include phrases, names, or other types of dictionary words.

Security Patch: A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most Mobile Devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

ENFORCEMENT: Any person found to be in violation of this regulation will be subject to appropriate disciplinary actions as defined by current college policy.

DR. CHARLES TERRELL, PRESIDENT

3/24/17
DATE

Approved by Technology Committee 9/1/2016

Approved by IET 2/6/17

Approved by President's Cabinet 2/28/17

14 day comment period 3/9/17 – 3/22/17