Allegany College of Maryland

MOBILE DEVICE POLICY

Adopted date 11/14/2018
Revised Date 6/20/2022
Reviewed by ITAC 11/14/2018
Implementation Date 11/14/2018
Type of Standard: Operational

BACKGROUND AND PURPOSE

The purpose of this standard is to define appropriate security measures that must be implemented on mobile devices that are used to access the data and resources residing at Allegany College of Maryland.

STANDARD

I. SCOPE OF THIS STANDARD

This standard applies to all faculty, staff, affiliates, and student workers who choose to use a mobile computing device, regardless of who owns the device, to access, store, or manipulate institutional data.

II. DEFINITIONS

Endpoint Security – Antivirus software sold by vendors like McAfee and Norton can be used to protect mobile devices from adware, viruses and malware.

Secure Wireless Network - the network encodes a message so that it can be read only by the sender and the intended recipient. Many public networks do not use secure encoding to protect communications. When accessing College resources, it is recommended that users limited their use of public networks. Examples: coffee shop Wi-Fi, restaurant Wi-Fi, hotel Wi-Fi, conference Wi-Fi.

Root or Jailbreak, - modify (a smartphone or other electronic device) to remove restrictions imposed by the manufacturer or operator, e.g. to allow the installation of unauthorized software.

Protected College Data – data that is protected by federal or state laws. Including: FERPA, HIPAA, and GLBA.

III. STANDARD STATEMENT

General Security

- Personal mobile devices are allowed for business use; however, they must meet all the standards outlined in college policies, and procedures regarding access to institutional technology resources.

- College owned mobile devices used at home should never be used for personal reasons and should never be used by other family members. Do not share College usernames and passwords with anyone.

- Mobile devices should be kept with users at all times or stored in a secured location when not in use. Mobile devices should not be left unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).

- Device operating systems must be kept up-to-date and endpoint security solutions should be deployed to protect the device from adware, viruses, and malware.

- Mobile devices should be password protected and auto-lock or screen timeout should be enabled.

- Devices that are “rooted” or “jailbroken” will not be allowed to access College data resources.

- Lost, stolen, or misplaced mobile devices that may contain protected college data should be reported to the Office of Information Technology via the helpdesk security breach form so that a "remote wipe" of the device can be initiated.

Transmission Security

- Where possible, data transmissions from mobile devices should be done over a secure wireless network.

- Wireless access, such as Bluetooth, Wi-Fi, etc., to mobile devices should be disabled when not in use to prevent unauthorized wireless access to the device.

Application and Data Security

- A personal device owner who installs College owned applications on their mobile device must agree to enable a “remote wipe”. A “remote wipe” will only remove College owned apps and data.

- A device owner must securely delete College owned programs and data from mobile devices before they are replaced or disposed of when a “remote wipe” is not enabled on the device.

- The College’s Security Policy does restrict the storage of protected college data on mobile devices.

- Software from unknown sources should not be installed on College owned or personal mobile devices as they may include software harmful to the device. Research the software intended for install to make sure that it is legitimate and safe.

IV. Enforcement

Users found to have violated this standard may be denied access to College computing resources and may be subject to other penalties and disciplinary action, both within and outside of the College. Any corrective measures taken shall be administrated in accordance with appropriate disciplinary procedures applicable to the relevant user.

V. Related Policies and Standards

Technology Resources Policy, Wireless Network Security Policy, Breach Notification Policy, Breach Reporting Procedures

VI. Administration of Policy

The office of the Dean of Information Technology, in consultation with The Vice President of Finance and Administration, shall be responsible for maintaining this policy.

VII. Changes

Substantive changes to this policy require approval by the Board of Trustees; editorial changes, title/position changes, and/or changes to its implementation procedures may be made as required by federal or state mandate and/or institutional need with timely notice to students and employees.