Washtenaw Community College

Mobile Device Policy

AN ADMINISTRATIVE INFORMATION SECURITY POLICY

PURPOSE

The purpose of this policy is to establish the requirements for the use of mobile computing devices at Washtenaw Community College. Mobile devices are important tools for the College, however they also represent a significant risk to information and data security. These requirements are necessary to protect College resources and preserve the integrity, availability and confidentiality of the College's information assets.

SCOPE

This policy applies to all employees who own or operate a mobile device that make use of applications which communicate with Washtenaw Community College's network, access College email, or store College data in any way, e.g. Blackboard, OneDrive, Google Drive, or other cloud storage service. This includes both personally owned and College-owned devices. Mobile devices include, but are not limited to, smart phones, tablets, watches, laptop computers, portable storage devices such as memory sticks, zip or flash drives, etc. In general, think any mobile device which can store or access College data.

ROLES & RESPONSIBILITIES

Information Security Office: The Information Security Office is responsible to ensure compliance with this policy as a component of the College's information security program.

Help Desk: The ITS Help Desk provides information and technical assistance to members of the College community in support of this and other Information Security policies.

Users: All Mobile Device users agree to comply with this policy and apply safeguards to protect Washtenaw Community College information assets from unauthorized access, viewing, disclosure, alteration, loss, damage or destruction. Appropriate safeguards include protection of their access credentials and the use of discretion in choosing what and where College Data is stored.

REQUIREMENTS & PRACTICES

Washtenaw Community College seeks to protect mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal. Mobile devices must be appropriately secured to prevent sensitive data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the computing and information infrastructure.

All users of mobile devices connecting to College networks or resources shall adopt the following practices:

- Employees shall first check with their supervisor prior to using a college-issued or personal device to access College resources. Supervisors shall remind employees of their responsibilities under this policy.
- Mobile devices should not be used to store confidential information as defined within the College's *Data Classification Policy*
- Mobile devices should be configured to require one of the following to gain access to the device:
  - A password in compliance with the College's *Password Complexity & Management Policy*;
  - A biometric identifier;
  - A PIN (minimum of 6 characters); or
  - A swipe gesture (minimum of 6 swipes)
- A mobile device must automatically lock and require one of these authentication methods for re-access after 5 minutes of idle time
- Mobile devices should be kept on the owners' person whenever possible

- Unattended mobile devices should be locked, physically secured and stored in secure locations, preferably out-of-sight
- Avoid lending mobile devices to others, and if you must, enable guest or guided access features to restrict access to applications and device settings
- Mobile devices configured to be utilized as part of any two- or multi-factor authentication should be configured to disable notification messages from appearing on the lock screen
- The device authentication setting must be changed if confirmed or suspected that it has become known to any third party

Users of mobile devices used to access, transmit, or store any sensitive College data (see *Data Classification Policy*), including such data contained within email message content accessed from the device, shall adhere to the following:

- In the event that there is a business need and no alternative to mobile device use, all confidential and other sensitive information stored, received or transmitted on a mobile device must be protected using strong encryption
- All College-issued mobile devices must be encrypted
- Note that College Data created or stored on a User's personal computers, smart phones or other mobile devices can be subject to freedom of information requests, subpoenas, court orders, litigation holds, and discovery requests
- Mobile laptop and tablet devices are expected to be configured in accordance with the College's *Computer & Server Security Standards*
- Ensure that any sensitive data inappropriately received is deleted and the sender and the Information Security Office notified. This can include situations of being an unintended recipient, or cases where confidential data is observed being stored or transmitted on mobile devices.
- All remote access to College information resources via mobile devices must adhere to *Remote Access Policy*
- Whenever possible, mobile device's should make use of automatic wipe functionality to securely erase the device after a sequence of no more than ten (10) unsuccessful attempts to unlock the device

- Whenever possible, mobile device's should make use of remote wipe features which permit a lost or stolen device to be remotely securely erased
- A college-issued mobile device is the responsibility of the employee to whom the device has been assigned
- The loss or theft of a mobile device used to access or store sensitive College data must be reported to the Information Security Office immediately
- Ensure that services that expose you mobile device to external connection, e.g. Bluetooth and Wifi hotspot, are configured securely with appropriate authentication
- Supervisors should coordinate with the Help Desk to ensure the following actions are performed whenever an employee separates from the College:
    - Access to any important work-related data or credentials which may be stored or accessible on the mobile device or known only to the departing employee is preserved and secured
    - A College owned mobile device must be returned to the supervisor or ITS immediately upon termination or resignation
    - A Personally owned mobile device which may have had access to College resources or data must have all College data, email, software applications and any account credentials erased

COMPLIANCE

This policy is a component of Washtenaw Community College information security program that is intended to comply with the PCI-DSS, FERPA, GLBA, HIPAA and other regulations.

EXCEPTIONS

The Chief Information Officer (CIO) or a designated appointee is authorized to make exceptions to this policy. Any requests for exceptions shall be made using the *Request for Policy Exception* form and a copy maintained by the CIO.

VIOLATIONS

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Washtenaw Community College reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity.

DEFINITIONS

Confidential Data: Specifically restricted data from open disclosure to the public by law is classified as Confidential Data. Confidential Data requires a high level of protection against unauthorized disclosure, modification, transmission, destruction, and use.

Data: Information collected, stored, transferred or reported for any purpose, whether electronically or hard copy.

Strong Encryption: Strong encryption is provided by well-established encryption algorithms, e.g. AES, SSL, which utilize long cryptographic keys, typically 256 bits or longer.

Strong Password: A password that is reasonably difficult to guess in a short period of time either through human guessing or the use of specialized software.

User: Any Washtenaw Community College faculty, staff, students or partner who has been authorized to access any College electronic information resource.

REFERENCES

Data Classification Policy

Password Complexity & Management Policy

Computer & Server Security Standards

Request for Policy Exception

REVISION HISTORY

Version	Description	Revision Date	Review Date	Approver
1.0	Initial version	10/11/18	-	WJO