**University of Maryland University College**

**Office of Information Technology**
**Wireless Device Guidelines**

## I. Introduction:

The University of Maryland University College (UMUC) may provide employees with wireless communication devices to enhance productivity and to maintain voice and data communication with staff providing critical support service to the University. Wireless devices shall be issued upon the approval of the Vice President for Information Technology Services or his/her designee. The following guidelines will apply to provisioning of wireless communication devices, with the full understanding that they are provided primarily for business use in accordance with UMUC's Acceptable Use Policy (http://www.umuc.edu/policies/fiscalpolicies/fisc27000.cfm). Exceptions to these guidelines may be requested in writing by the appropriate Cabinet member to the Chief Business Officer (CBO).

## II. Approval Criteria:

Smart Phone

The employee for whom the device is requested must meet one or more of the following criteria:

- The employee is required to work evening/weekend/on-call hours and requires e-mail communication; or there is a frequent need to contact the employee after normal work hours via e-mail.

- There is a need for the employee to regularly have e-mail contact with other employees after normal business hours; or the employee frequently spends most of his/her work day away from his/her office and there is a need for the employee to be in constant e-mail contact during normal business hours.

Cell Phone

The employee for whom the device is requested must meet one or more of the following criteria:

- The employee frequently spends most of his/her work day away from his/her office and requires voice communication; or the employee is

required to work evening/weekend/on-call hours and requires voice communication.

- There is a frequent need to contact the employee after normal work hours via telephone; or there is a need for the employee to have telephone contact with other employees after normal business hours.

Broadband Card Access

The employee for whom the device is requested must meet one or more of the following criteria:

- The employee is required to be on-call to support mission critical activities where internet access is required.

- The employee is frequently required to make off-site presentations requiring internet access to groups, organizations, or others regarding UMUC programs/events/activities for enrollment, recruitment, fund raising and similar activities identified by their functional area.

Tablet Device

The employee for whom the device is requested must meet one or more of the following criteria:

- The employee is required to be on-call to support mission critical activities where e-mail and internet access is required, specific applications are required, and/or and a Smart Phone is not adequate.

- The employee is frequently required to make off-site presentations requiring internet access to groups, organizations, or others regarding UMUC programs/events/activities for enrollment, recruitment, fund raising and similar business activities.

- There frequently is a need to contact the employee after normal work hours via e-mail; or there is a need for the employee to be in constant e-mail contact during normal business hours, specific applications are required, and/or a Smart Phone is not adequate

**III. Administration of Guidelines:**

1. Requests:

All requests for wireless devices shall be made by IT Liaisons on behalf of the employee requesting a wireless device, with approval from the employee's supervisor, utilizing the Information Technology eRequest System. The completed form will require a stated business purpose supporting the request along with the specific device being requested. Multiple devices providing comparable functionality will be issued only on an exception basis. All requests will be reviewed by the Vice President for Information Technology Services or his/her designee who will apply the approval criteria to the request and either approve or deny the request.

Approved requests will be forwarded to the IT Wireless Coordinator for provisioning.

2. Provisioning

The IT Wireless Coordinator will verify specific plan requirements with the approved end user to ascertain the appropriate plan for the intended use taking into consideration voice minute plans, data plans, etc.

The device will be provisioned and activated by IT staff.

The end user will be required to sign a responsibility statement - Wireless Device Lending/Terms of Use Agreement - when accepting the device and agree to UMUC's use policies.

Devices with voice plans will be issued with Bluetooth devices to enable "hands free" operation by request. The end user is personally responsible to comply with state laws regarding the use of wireless devices while driving a motor vehicle, and also must comply with the Governor's Executive Order regarding use of wireless devices while driving State owned vehicles or while driving on State/UMUC business.
(http://www.dsd.state.md.us/comar/comarhtml/01/01.01.2009.08.htm)

3. Customer Service

The IT Wireless Coordinator will be responsible for providing training on the operation of the device(s) issued.

Requests for service will be directed to the IT Wireless Coordinator who will be UMUC's primary liaison with the vendor on matters relating to repair and warranty service.

Wireless devices will be upgraded in accordance with the contracted plan terms and conditions. It will be the responsibility of the IT Wireless Coordinator to collaborate with the end users to maintain currency of devices. The IT Wireless Coordinator will be responsible to standardize the devices deployed and coordinate their selection with other support units with IT such as the Service Desk and the Technical Support Group.

4. Roaming/Short Term Use

All devices will be deployed as domestic use devices; international calling and data plans may only be provisioned upon approval of the Vice President for Information Technology Services or his/her designee. International use, if permitted by the functional area senior leadership will be subject to limitations. This requirement applies to all cell phones, smart phones, tablet devices, or other communication technology that may be made available to end users. In the event that permission is not first obtained, the end user may be personally liable for any and all charges that UMUC may incur as a result of unauthorized use.

International service for broadband/modem cards and tablets will not be provisioned due to excessive cost. Individuals traveling internationally are encouraged to use publicly available WiFi connectivity, subscribe to Internet service at their hotel, or rely upon other wireless devices to access the internet.

5. Features
The devices are to be primarily used for UMUC business purposes. International roaming is prohibited except by approval of the Vice President for Information Technology Services or his/her designee and for UMUC business travel only (except those issued to Executive Committee members who regularly require roaming privileges).

Applications can be purchased and downloaded to UMUC devices if they have a valid business purpose. Applications must be paid via the end user's personal credit card and submitted for approval for reimbursement to the end user's department head. UMUC P-Cards cannot be used to purchase applications.

6. Security

UMUC devices require password protection by the AirWatch Agent mobile management app. End users are prohibited from sharing password information with any other individuals and will comply with UMUC password standards.

Lost or stolen devices are to be reported immediately to the IT Service Desk at 301-985-7400 or servicedesk@umuc.edu. The Office of Information Technology will typically disable and wipe all data from lost or stolen University-owned devices.

**IV. Compliance:**

1. The IT Wireless Coordinator will review invoices for wireless service monthly to monitor and report overages for voice and data plans, roaming charges, and other additional fees and costs assessed each individual plan. Variances shall be reported to the Assistant Director, IT Business who will validate the business use/necessity for the overages with the end user's department head.

2. The IT Wireless Coordinator shall also monitor individual invoices to determine if the device is being used sufficiently to merit deployment and will report this information to the Assistant Director, IT Business who shall follow-up with the respective department head.

3. The IT Wireless Coordinator will also scrutinize monthly invoices to detect potentially abusive use of the device and report that to the Assistant Director, IT Business for further review.

4. Use of the device(s) must be in compliance with all applicable federal, state, local, and international (where applicable) laws, regulations, and executive orders including, those that restrict the use of cell phones and/or text messaging devices while operating a motor vehicle

**V. Use of Personal Devices on the UMUC Network:**
Employees who wish to use a personal mobile device to access University services, such as e-mail or the UMUC network, are required to safeguard University data and personally identifiable information. UMUC requires that the AirWatch Agent mobile management application be installed on their device as this will allow UMUC access and permission to delete University data if the device is lost or stolen or no longer being used by the employee for any reason, including separation from employment. UMUC retains the right to delete University data, accounts and applications from any wireless device that contains the University's information.

UMUC requires that all users connecting personal mobile devices to the UMUC network and other University services adhere to required security policies for those devices at the time connected and any updates to the policy thereafter. This includes UMUC's Acceptable Use Policy (http://www.umuc.edu/policies/fiscalpolicies/fisc27000.cfm).

If an employee's device is lost or stolen, the employee must contact the IT Service Desk at 301-985-7400 or servicedesk@umuc.edu immediately. The Office of Information Technology will typically provide owners of personal devices the option of deleting only University data or all data from a lost or stolen device.

If an employee begins to utilize a replacement personal mobile device, the employee must install AirWatch on the new device.

**Terms and Conditions**

All users must acknowledge and agree that:

- Users of personal end user devices shall not circumvent security controls designed to protect UMUC information resources.
- UMUC is not liable for any damages, including data or functionality losses, of an end user device that it authorizes an employee or contractor to use in the performance of his or her duties.
- Personal mobile devices will not be used as the sole or principal storage for UMUC records.
- Any personal mobile devices accessing e-mail or other UMUC services must have the AirWatch Agent app configured to protect University data. When an end user device is no longer used to access UMUC resources, the user will permit UMUC to permanently remove any UMUC records, including any sensitive data stored on the device.
- Employees must immediately report the loss or theft of their connected mobile device to the UMUC IT Service Desk; the user agrees that UMUC may take whatever measures necessary to permanently remove any UMUC records, including any sensitive data stored on that device.
- While connected to the UMUC network, UMUC has the right to monitor the end user mobile device and to investigate reported incidents of suspected abusive and/or illegal activities on those devices. The investigations may include reviews of electronic data files and records and may require confiscation of the personal equipment.
- All users acknowledge and agree that a violation of any of these terms and conditions may result in appropriate disciplinary action, up to and including termination of employment.