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 UMGC 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 UMGC 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 email 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 ø⅄ℕŜfŜăă ŘŜØ⅄ŎŜΣ ø⅄ûK I·LJLJℕ⇄ØI·f ₹ℕ⇄Y ûKŜ ŜY LJf⇄èŜŜΩă ădzLJŜℕØ⅄ă⇄ℕΣ dzûλfλÎλy∃ ûKŜ Ly₹⇄ℕY I·û⅄⇄y ¢ŜŎKy⇄f⇄∃è 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 UMGC [illegible] est. 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 [illegible] vehicles or while driving on State/UMGC 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 [illegible] 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 UMGC 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 UMGC business purposes. International roaming is prohibited except by approval of the Vice President for Information Technology Services or his/her designee and for UMGC business travel only (except those issued to Executive Committee members who regularly require roaming privileges). Applications can be purchased and downloaded to UMGC devices if they have a [illegible]

ŦŽNJ I·LJLJNJŽØI·f ŦŽNJ NJŜλY˘ōdzNJăŜY˘Ŝyű ű2 űKŜ ŜyŘ dzăŜNJΩă ŘŜLJI·NJűY˘Ŝyű KŜI·Řφ ¦ a GCP-Cards cannot be used to purchase applications.

6. Security

UMGC 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 UMGC password standards. Lost or stolen devices are to be reported immediately to the IT

UMGC requires that all users connecting personal mobile devices to the UMGC 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 UMGC's ! ÕÕŜLJűl·ōfŜ ¦ăŜ t2fłÔè (http://www.umuc.edu/policies/fiscalpolicies/fisc27000.cfm).

LF l·y˝ŜY˙LJf2èŜŜ⍺ă ŘŜØłÔŜ łă f2ăú 2№ ăú2fŜy˘ úKŜ ŜY˙LJf2èŜŜ Y˙dzăú Ô2yűl·Ôű úKŜ L¢ {Ŝ№ØłÔŜ 5Ŝă⌋ l·ú олм-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 UMGC information resources.
- UMGC 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 UMGC records.
- Any personal mobile devices accessing e-mail or other UMGC services must have the AirWatch Agent app configured to protect University data. When an end user device is no longer used to access UMGC resources, the user will permit UMGC to permanently remove any UMGC records, including any sensitive data stored on the device.
- Employees must immediately report the loss or theft of their connected mobile device to the UMGC IT Service Desk; the user agrees that UMGC may take whatever measures necessary to permanently remove any UMGC records, including any sensitive data stored on that device.
- While connected to the UMGC network, UMGC 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.