I. POLICY STATEMENT

The following policy applies to institutionally procured mobile devices and mobile services.

- Manager/Supervisor must approve all employee requests for purchase of mobile device and/or mobile service.
- Mobile Devices will be limited to pre-approved standard models established by UMass Lowell’s Information Technology Department.
- Mobile services will only be provided by accepted University plans and carriers.
- Employees will use mobile devices in accordance with UMass Lowell’s Acceptable Use Policy and Mobile Device Security Standards document.
- All eligible employees who are provided mobile service will be reported on, and taxed if applicable, in accordance with University policy and/or IRS regulations.

II. PURPOSE

The purpose of this policy is to establish a framework for consistent decision-making regarding the provision of essential, business-related mobile devices to university faculty and staff. University leadership intends that this policy, and its associated procedures and standards, will promote compliance with IRS requirements and will manage the risks and administrative burdens associated with the use of mobile devices to facilitate University business. Specifically:

- Ensure mobile service is distributed to employees where the associated benefits justify the expense.
- Ensure mobile devices selected for initial procurement are associated with the approved business justification.
- Ensure mobile devices selected for initial procurement are procured by UMass Lowell and are selected from a predefined list of standard equipment.
- Prevent unexpected and unacceptable charges and fees.
- Properly report and tax personal use, if applicable, of UMass Lowell funded mobile devices in accordance with IRS guidelines.
- Ensure all mobile devices capable of storing university data have proper university security controls in place in accordance with the Mobile Device Security Standards document.
- Ensure all mobile devices no longer in use follow the disposition procedures in accordance with the UMass Lowell Sanitation and Disposal of Information Resources Policy.
III. SCOPE

This policy applies to all eligible UMass Lowell employees who utilize mobile devices to access, transmit, and/or store university data. For the purposes of this policy, mobile devices include tablets and smartphones such as (but not limited to) all iOS devices (iPhones, iPads, iPod Touch), Android devices (both phones and tablets), and Windows mobile devices. It does not include laptops.

IV. DEFINITIONS

Mobile Telephone: A portable device that connects to a mobile network for the provision of voice, text, and messaging services, as well as (in some cases) data connectivity.

Smartphone: A type of mobile telephone that has data connectivity for email access, calendar management, and web browsing capabilities, as well as the capability to run numerous applications.

Mobile Device: A portable device that connects to a mobile network for the provision of voice, messaging, and/or data services. Examples include all iOS devices (iPhones, iPads, iPod Touch), Android devices (both phones and tablets), and Windows mobile devices. It does not include laptops.

Senior Leadership Team (SLT) Member: The most senior leader of one or more operational units, that reports directly to the Chancellor.

Device Manager: The individual that has stewardship responsibility for the mobile device, mobile telephone, and smartphone of the department, as delegated by a member of the Senior Leadership Team.

University-owned device: A mobile device purchased and owned by the University that connects to a mobile network through a University-sponsored plan.

University-sponsored plan: A contract between the University and a mobile service provider to provide voice, messaging, and/or connectivity to a University-owned device.

Personal mobile plan: A contract between an employee and a mobile service carrier to provide voice, messaging, and/or data services to a personally-owned mobile device.

Device Applications (Apps): A self-contained piece of software designed to fulfill a particular function. For the purposes of this policy, the definition applies as, downloaded by the user to a mobile device.

V. PROCEDURES

A. Eligibility to Receive a University-Owned Device

Each department head (Device Manager) determines if an employee is eligible to receive a University-owned device. Eligibility criteria include:

a. Employee is required to respond to emergency calls from the University after hours; and
b. Employee is often working away from the desk phone and routinely needs to be
c. Employee uses mobile devices routinely and with regular/high volume to respond to University emails (during normal and non-business hours) and to make business phone calls.
d. Employee monitors and administers mission critical information systems during non-business hours.

B. Requesting Mobile Devices

Employees and/or Departments may request a mobile device or service by creating an IT Service Request via http://helpdesk.uml.edu. This request should justify the expense to UMass Lowell.

Because of initial and ongoing costs and short product lifecycles, employees and/or departments will be provided the most cost effective mobile device and service from university-approved devices and plans that fulfill their approved business need.

*Exceptions to the university-approved device list and/or plan MUST be approved by the Vice Chancellor of Finance and Operations.*

The process for equipment upgrades, including changes to International voice and/or data plan is:

- Request is submitted to Information Technology by creating an IT Service Request via http://helpdesk.uml.edu.
- Information Technology processes requests and verifies upgrade eligibility.

C. Acceptable Use and Business Practices

- Mobile devices and services will be paid directly by UMass Lowell.
- Mobile devices procured using personal funds will not be reimbursed by UMass Lowell.
- Reimbursement for expenses associated with a “personal mobile plan” or personal mobile phone is not permitted. Exceptions must be approved by an SLT member.
- Downloading and/or using fee-based services (Apps) not originally requested are not permitted. Examples include custom ring tones, GPS programs, premium text services, games, etc.
- Maintaining two active mobile devices or more per employee (e.g. two phones, one phone and one tablet, two air cards) is not permitted unless there is a written and approved business justification by their SLT member.
- Mobile device selection will only be allowed from university-approved models.
- Mobile service will be provided under University-approved plans only.
- Replacing mobile devices prior to upgrade eligibility is not permitted.
- Mobile device upgrades will only be allowed under the following conditions:
  - Upgraded is available under the existing contract but no sooner than once every thirty (30) months.
  - Upgrade to a university approved model one-step below the most current release.
- Replacement of lost, stolen or damaged mobile devices occurs when reasonably necessary. If an employee fails a reasonable standard of care for devices, it is the immediate supervisor’s decision to replace the employee’s device. The employee
must secure approval from their direct supervisor for a replacement device prior to initiating the replacement transaction with Information Technology.

- Changing carriers or equipment for personal convenience is not permitted.
- Incurring International voice and/or data charges is not permitted; International plans must be requested one business week prior to travel.
- Maintaining devices that are idle for more than 90 days will result in the service plan’s cancellation.

Unacceptable use of mobile service may result in loss of device privilege, disciplinary action and institutional reimbursement of the amounts charged plus applicable fees and taxes.

D. Retention of Personal Telephone Numbers Used on University-Managed Accounts

Employees that wish to assign, and later retain, a personal mobile device number to a University-managed account must make this known when initiating service. The University cannot guarantee that the employee will be able to retain the telephone number on termination of employment.

Reassignment of a personal number from a University-sponsored account to a personal account must occur at the time of cessation of employment.

VI. RESPONSIBILITY

Information Technology is the responsible organization for implementing the provisions of this policy on behalf of the Vice Chancellor of Finance and Operations. The University’s Chief Information Officer and the Information Security Officer are the designated points of contacts. At the department level, specific responsibilities include:

- **Employee**
  - Sign the Mobile Device Acceptance form and complete the IT Service Request for a mobile device.
  - As with any device that has the capability to store data, or access data via the University network or the internet, the employee must adhere to University data security policies and standards.
  - Maintain a current backup of the device to prevent the possible loss of data.
  - Return all university-owned mobile devices to Information Technology upon discontinuance of use (i.e. device upgrade) or departure from University employment for proper disposal and/or reassignment.

- **Department Head/Supervisor and/or Device Manager**
  - Provide employee with Mobile Device Policy.
  - Provide business justification and approve the Mobile Device Request.
  - During off-boarding process, coordinate with departing employee to collect university-owned mobile devices and computing resources, and return to Information Technology for dispositioning.
  - Annually review existing devices/services to ensure they are needed and represent the best options (most economical) given their business use.
• Information Technology
  o Coordinates the purchase of mobile devices, accessories, service changes, and modifications via online portal.
  o Provides a 24/7 service desk for mobile device support.
  o Maintains inventory of mobile devices and upgrade eligibility.
  o Monitors mobile device plans and overage charges and suggests/implements cost saving changes.
  o Informs employee mobile device is ready for pickup and provides set-up, data migration and training services.
  o Collects, wipes and disposes of all decommissioned university owned mobile devices.
  o Maintains the mobile device policy forms acknowledging receipt of device.

VII. ATTACHMENTS

Mobile Device Acceptance Form

VIII. RELATED POLICIES, PROCEDURES, AND ANNOUNCEMENTS

Acceptable Use Policy, IT-5-101
Sanitation and Disposal of Information Resources Policy, IT-5-107
UMass Lowell Mobile Device Security Standards

IX. APPROVAL AND EFFECTIVE DATE

On file with the Policy Office.
Mobile Device Acceptance Form

I accept and understand that mobile devices and/or accessories provided for my use are the property of the University of Massachusetts. I agree to abide by the terms of the UMass Lowell Mobile Device Policy (http://www.uml.edu/IT/Policies).

It is the policy of the University of Massachusetts Lowell that when an employee terminates employment the mobile device is left with the employee’s supervisor/manager or HR representative for proper dispositioning with Information Technology.

I accept and understand that I will be held responsible for the loss of the mobile device while in my possession. I will immediately notify Information Security in the event of loss or theft, and will immediately file a police report with the University Police.

I accept and understand that Information Technology reserves the right enforce the security settings as stated in the Mobile Device Policy, and to wipe (erase) the data on the mobile device in the event of loss or theft.

I understand that a violation of the terms and conditions set out in the UMass Lowell Mobile Device Policy may result in the restriction and/or termination of my use of University issued mobile devices, equipment, and/or accessories and may result in further discipline up to and including termination of employment and/or other legal action.

Employee Printed Name: ____________________________  Date: _____________________

Employee Signature: ________________________________