MDM Guidelines

I. Purpose

The purpose of these guidelines is to establish mobile device management standards for securing college owned mobile devices. College owned devices are defined as any smart device running iOS, Android, Windows RT operating systems. Effective implementation of these standards will allow to manage mobile devices with a centralized enterprise application.

II. Scope

The guidelines apply to all mobile devices purchased by the college with a South Texas College inventory asset tag. All mobile devices that are connected to a wireless network can be managed on and off premises.

III. Privacy

Mobile Internet devices can have profound privacy implications. Almost all mobile Internet devices may have their physical location tracked via GPS or other means. STC Technology Resources Department does not collect or monitor any data stored on your mobile device or your mobile device location, unless the device has been reported lost or stolen, or is part of an ongoing investigation.

IV. Guidelines

A. Ownership and Responsibilities

Custodian

- The responsible party for the safety and security of the assigned mobile device.

The assigned user of the mobile device

The Department of Technology Resources is responsible for the safety and security of data on its network and the equipment used to run the network infrastructure.

- Users must ensure that they comply with all sections in this agreement. Users must agree to take shared responsibility for the security of their mobile devices and the information they contain.
- Mobile devices are issued for business purposes and remain the property of South Texas College.
- When the mobile device is allocated, the user assumes responsibility for the physical security of the equipment and information contained within.
- Prior to South Texas College allocation of a mobile device, the user must review and sign this policy document and the user agreement.
- Users are not permitted to authorize purchases or services for their mobile devices.

B. Loss or Theft

- It is the user's responsibility to take appropriate precautions to prevent damage to or loss/theft of the device.
- If the device is lost, stolen or suspected to be compromised in any way, the user must notify the help desk immediately if possible or within twelve (12) hours maximum. This notification must take place prior to any cancellation of mobile voice and data services associated with the device.

C. Applications and Downloads

- Users must take all reasonable steps to protect against the installation of unlicensed or malicious applications.
- All software on the device must either be provided and installed by South Texas College or approved by South Texas College for installation by the user. A list of permissible software applications is available at [insert intranet URL]. Users should understand that unmanaged or unapproved installations not only compromise the operating environment, but also constitute a security risk, including the intentional or unintentional spreading of software viruses and other malicious software.
- Downloading applications from the platform (for example, Apple, Android) general application store is acceptable, as long as the application complies with this policy, as well as the IT security policy and HR policies of South Texas College, and is not on the blacklist at [insert app store or intranet URL], or the app is available on the whitelist at [insert app store URL].
- Unless previously approved, South Texas College credit cards may never be used for app store purchases nor entered into an app store account. Any authorized app store purchases must be made through the use of a volume purchase license, or paid individually by the user, and subsequently submitted in an expense report for reimbursement.
- Commercial software (including shareware) must have a valid license for each prospective user, and must be validated, approved and installed by IT security.
- Users are not permitted to make copies of licensed software.
- Users must ensure that they comply with data copyright requirements.
- All South Texas College-owned devices, including, but not limited to, South Texas College-issued iPads, must be connected exclusively and without exception to South Texas College-owned PCs in order to use iTunes or equivalent software. South Texas College-owned devices are to never be connected to non-owned PCs for accessing iTunes or equivalent software.
- Personally owned devices should not be connected to enterprise-owned PCs to utilize any consumer media technology such as iTunes.

D. Functionality and Feature Management

The device OS must be used "as is." The device functionality must not be modified, unless required or recommended by South Texas College. The use of devices that are jail-broken, "rooted" or have been subjected to any other method of changing built-in protections is not permitted, and constitutes a material breach of this policy.

At South Texas College request, users are responsible for delivering the mobile device to the IT security department if and when the device is selected for a physical security audit, or is needed for e-discovery purposes.

If the mobile device is lost, stolen or compromised, or when an employee is separated from the company through resignation, termination or layoff, the enterprise has the right to secure enterprise data by wiping the device. Before this occurrence, the user is solely responsible for backing up any personal content on the device.

E. Technology Resources Responsibilities and Procedures

The IT organization's responsibilities include:

- Publishing IT standards that document the type of organization-owned mobile devices approved for use for/connection to South Texas College IT resources, including specific requirements governing the equipment's configuration/controls and connection/operational charges
- Making users aware of any changes to technologies or policies that will impact daily use
- Ensuring that applications are available and optimized for devices
- Handling operating management functions that control organizational information assets on devices

F. Approval and Delivery to Client(s)

Approved purchases for mobile devices will be shipped from the vendor to Shipping and Receiving. The devices will be forwarded to Technology Resources for pre-deployment configuration. Once device(s) are configured with the College's mobile device management software and approved applications, the device will be sent to the client. Clients requiring specific applications or custom configurations must submit a request to Technology Resources prior to purchasing the mobile device.

The current software baseline for College-owned mobile devices is:

- AirWatch Mobile Device Management software
- McAfee anti-virus Software (If applicable to device)
- JagMobile mobile application
- Microsoft Office suite (if applicable to device)

Mobile Application Purchases

Mobile application purchases will be approved through Technology Resources, purchased through a centralized account and deployed to the device via AirWatch Mobile Device Management. For assistance with mobile application purchases, please contact Technology Resources [contact person/department].

Supervisor Responsibilities

The supervisors' responsibilities include:

- Distributing and communicating policies, standards and guidelines to their staff
- Enforcing and ensuring compliance with all policies and standards
- Approving the use of organization-owned mobile devices by individuals under their supervision or areas of responsibility

Data and System Security

All South Texas College data that is stored on the device must be secured using South Texas College-mandated physical and electronic methods at all times. Mobile device users must comply with physical security requirements when equipment is at the user's workstation, and when traveling. All users must take the following physical security preventative measures defined in [reference appropriate organization document] to protect South Texas College data and systems:

- Users shall abide by South Texas College standard information security directives for the device at all times.
- Users must comply within [define time frame, in number of hours or days] with directives from their business units to update or upgrade system software, and must otherwise act to ensure security and system functionality.
- All mobile devices connecting to the network must meet the security criteria defined in Appendix A.
- Mobile devices must not be left in plain view in an unattended vehicle, even for a short period of time and must not be left in a vehicle overnight.
- Mobile devices must be positioned so that they (and the information contained within them) are not visible from outside a ground-floor window.
- A mobile device displaying sensitive information being used in a public place (e.g., train, airplane or coffee shop) must be positioned so that the screen cannot be viewed by others, thus protecting South Texas College information. A tinted or polarized screen guard may be used to decrease the viewing angles of any mobile device.
- When leaving a mobile device unattended for any extended period (for example, on lunch breaks or overnight), users must physically secure it. Another option is to lock the device in a cabinet, or to lock the door of an individually occupied office.
- In vulnerable situations (e.g., public areas such as airport lounges, hotels and conference centers), the mobile device must not be left unattended under any circumstance.
- Portable computers and devices should be carried as hand luggage when traveling, and should never be checked as baggage or luggage to be stored anywhere, thus prohibiting immediate access or visual contact with the device.
- When returning the mobile device for an upgrade or upon termination of employment, users must confirm the removal of any enterprise data and any backups thereof, before any payment of severance, pension or other compensation can be dispensed.

Password Protecting Mobile Devices

Physical security is a major concern for mobile devices, which tend to be small and easily lost or misplaced. The security of your system is only as strong as the password you select to protect it. Review ISO guidelines for selecting a secure password. [REFERENCE POLICY HERE]

- **Strong Passwords**
  It is important to choose a strong, effective password that is not easily guessed for your mobile device. For assistance with selecting a strong password, please contact Technology Resources [contact person/department].

- **Antivirus/Anti-spam software**
  Mobile devices can be just as susceptible to viruses as desktop computers. A number of vendors offer antivirus and anti-spam solutions such as Airscanner, F-Secure, and Trend Mobile. For assistance with antivirus and anti-spam software, please contact Technology Resources [contact person/department].

Mobile Device Management and Monitoring

College-owned mobile devices will NOT be monitored by Technology Resources or College staff unless an incident is reported regarding loss, damage, theft of the device, or an ongoing investigation requiring access to device logs and/or data. Technology Resources staff will **NOT** access mobile devices without first contacting the user and obtaining consent. [REFERENCE POLICY HERE]

Reporting

Technology Resources will regularly collect and provide statistics to the College regarding the number of registered College-owned mobile devices and purchases/utilization of mobile applications purchased through College accounts from Apple iTunes, Google Play, or Microsoft App stores. Technology Resources will only report on the location of a College-owned mobile device if the device has been reported lost or stolen, or if the device is involved in an ongoing investigation.

Safe Disposal Practices

When you are ready to dispose of your device, be sure to remove all sensitive information first. Technology Resources can assist with wiping your device to ensure there is no sensitive data remaining prior to disposal. For assistance with device disposal, please contact Technology Resources [contact person/department].

. Status & Revision History

I hereby approve and authorize this process commence as of February, 10th, 2015.

Alicia Gomez, CIO	**Jose Lucio Gonzalez, ACIO**	**Ali Kolahdouz, ACIO**

Revision History

Date	Author	Description

Change Log

Version	Prepared/Modified By	Date
V1.0	Lucio Gonzalez, Steven Bourdon, Ali Kolahdouz	2013-12-02
V1.1	Lucio Gonzalez, Alicia Gomez, Ali Kolahdouz	2014-01-14
V1.2	Ali Kolahdouz	2014-07-09
V1.3	Air watch team	2015-02-10