THE CITADEL
The Military College of South Carolina
171 Moultrie Street
Charleston, SC 29409

MEMORANDUM 18 May 2017
NUMBER 3-607

MOBILE DEVICE DISTRIBUTION AND USE POLICY

1. PURPOSE

This policy outlines the processes and procedures associated with the distribution of cell phones and other mobile cellular devices to faculty and staff. The Citadel offers a taxable allowance for personal communication services (i.e. cell phone or wireless device) to employees whose duties and responsibilities require them to maintain such services.

2. REFERENCE

IRS Notice 2011-72

3. DEFINITIONS

A. Cell Phone: A mobile phone with limited functionality. A cell phone may include basic features such as a keyboard or rudimentary applications. It does not include internet connection capabilities, email access, or other "smart" features.

B. Smartphone: A mobile phone that includes features such as internet connectivity, Wi-Fi, e-mail access, applications and a web browser.

C. Tablet: Mobile devices usually consisting of a large (6"+) touch screen, internet connectivity and other "smart" features. A tablet typically does not include telephony services, although third-party applications may provide them.

4. POLICY

A. The appropriate Dean, Director, Vice President, or designee, may authorize employees whose job duties include the frequent need for a mobile device to receive either of the following:

1. A **stipend** for using an employee-owned device that has been authorized to access Citadel resources in relation to the employee's job duties. See Annex A.

Stipend amounts will be determined based on the business contact required of an employee's position and the data needed for the employee to perform his

or her job responsibilities (see Annex A for stipend amounts and Annex B for Allowance Guidance).

2. **Citadel-issued** cell phone, smartphone, and/or tablet.

   Devices purchased by The Citadel, regardless of the source of funds, are the property of The Citadel. Devices, accessories, and equipment must be accounted for as required by state law, and are to be turned in to the department when an employee transfers or terminates employment.

3. **Citadel-issued department** cell phone, smartphone, and/or tablet.

   Devices purchased and used by a department and rotated to appropriate "on-call" personnel. Responsible departments will appoint a responsible individual to track usage and appropriate care of device.

B. An employee is eligible for a **Citadel-issued** device or **stipend** if at least one of the following criteria is met:

   1. The job function of the employee requires considerable time outside of his/her assigned office or work area and it is important to The Citadel that s/he be accessible during those times;

   2. The job function of the employee requires him/her to be accessible outside of scheduled or normal working hours or in times of crisis;

   3. The job function of the employee requires him/her to have wireless data and internet access outside of scheduled or normal working hours or in times of crisis.

C. The allowance of employee-owned devices may require an opt-in decision that trades control over the employee-owned device in exchange for access to Citadel resources such as documents and email. For employees that are approved to use an employee-owned mobile device to conduct Citadel business **and** receive a stipend, the employee must:

   1. Purchase cellular phone service and equipment and comply with vendor terms and conditions;

   2. Select a service provider, plan, coverage area and features that meet the requirements of their responsibilities for The Citadel job and the level of service that the stipend is intended to cover; and ensure the carrier selected has service in required usage areas, such as on campus and/or at home as required by the department;

   3. Maintain an active service contract for the duration of the stipend;

4. Report any cell phone number or plan changes to supervisors and Information Technology Services within 24 hours;

5. Accept that the device may be remotely wiped (i.e. erasing all data and applications, including personal information) by The Citadel or accessed for legitimate business purposes; **The Citadel will only wipe data related to The Citadel but cannot guarantee that personal data will not be affected**;

6. Acknowledge that The Citadel is in no way responsible for damaged, lost or stolen employee-owned devices while the user is performing Citadel business; and

7. If requested by The Citadel, allow manageability software to be loaded and maintained on the employee-owned device.

D. Privacy.

The Citadel may need to access the employee-owned device for legitimate business purposes including, but not limited to implementing security controls, fulfilling record retention obligations, conducting investigations, or responding to litigation-related requests arising out of administrative, civil, or criminal proceedings. Employees are expected to provide access to their device upon request for necessary business purposes. The Citadel may also need to copy the entire device; including personal content to meet business obligations and it will not likely be able to differentiate between personal data and employer data at the time of collection.

1. Employee-owned device requirements:

   a. User will not download or transfer sensitive business data to an employee-owned device; this excludes Citadel email which is protected through the various security controls listed below;

   b. User will protect the device with a password or other form of user authentication;

   c. User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer; the user will not “jail break” the device by installing software that allows the user to bypass standard built-in security features and controls;

   d. User agrees that the device will not be shared with other individuals or family members, due to the business use of the device. (e.g., potential access to government e-mail, sensitive data, etc.);

e. User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments;

f. Upon request by The Citadel, the user must allow the installation of mobile device management software or any other software deemed necessary, on the user's device; and

g. User agrees to delete all Citadel data from the device when employment with the College terminates, except when required to maintain the data in compliance with a litigation hold notice.

2. Citadel-issued devices:

a. Citadel-issued devices are to be used for official use only, subject only to limited incidental personal use that does not increase The Citadel's cost or violate any laws or ethical standards; and

b. Employees have no expectation of privacy as to the use of Citadel-issued devices; The Citadel will have access to detailed records of mobile communication device usage, which may be subject to audit.

3. Employees who receive a Citadel-owned device or a stipend shall:

a. Assign an unlock password, passcode or Personal Identification Number (PIN) to prevent unauthorized use;

b. Configure the device to lock at startup and after no more than five minutes of inactivity;

c. Report any loss or theft to supervisor and Information Technology Services, if a phone is stolen or missing within 24 hours; and

d. Comply with all Federal and State data maintenance and protection laws (e.g., Family Educational Rights and Privacy Act (FERPA), records retention requirements), as well as all Citadel policies, including those pertaining to data security, acceptable computing use, email, etc.

5. COMPLIANCE

Failure to comply with this policy, depending on the level and intent of non-compliance, may result in any of the following: discontinuance of the stipend, reimbursement to The Citadel of previously paid stipends, revocation of access privileges, or disciplinary action up to or including termination of employment.

6. NOTES

A. Dates of Official Enactment and Amendments:

Approved by the Provost on 18 May 2017.

Non-substantive changes on 18 May 2017: added hyperlinks for cross-reference policies and consolidation of Annex A information; form is now a one-page. Fixed footers.

B. Responsible Department:

Information Technology Services

C. Responsible Official:

Chief Information Officer

D. Cross References:

Memorandum 3-2 Computer and Network Use Policy

Memorandum 3-3 Computing Resources Security Policy

Memorandum 3-4 Access to Electronic Mail Services

Memorandum 3-6 Electronic Information Security Policy

7. RESCISSION

Memorandum 3-607, dated 4 May 2017.

8. REVIEW

Review this policy on a biennial basis.

FOR THE PRESIDENT:

OFFICIAL

//Signed, CLB, 18 May 2017//
CONNIE L. BOOK, PhD
Brigadier General, SCM
Provost and Dean of The Citadel

Attachments
Annex A, The Citadel Mobile Device Stipend Agreement Form
Annex B, The Citadel Mobile Device Stipend Allowance Guidance

Annex A

The Citadel Mobile Device Stipend Agreement Form

Employee Name: _____ Stipend Start Date (next pay period): _____

Job Title: _____ Monthly Stipend: _____ Index: _____

Department Name: _____ Cell Phone #: _____ Cellular Carrier: _____

Stipend	Basic Cell	MiFi/iPad	Smartphone
Full	**$40**	**$10**	**$60**
Partial	**$20**	**N/A**	**$30**

Policy Summary

Employees who hold positions that include the need for a mobile device may receive a stipend to compensate for business-related costs incurred when using their individually-owned device. The stipend will be considered a taxable fringe benefit to the employee. The amount of the stipend will be determined by a person's job duties as they relate to use and access. The Citadel will review and revise the amounts to be provided for stipends and reimbursement on an annual basis.

Employee Responsibilities. Recipients of a mobile device stipend shall:

- Purchase cellular phone service and equipment and comply with vendor terms and conditions; the employee is responsible for plan choices, calling areas, service features, termination clauses, and paying all charges associated with the cellular service and device;
- Select a service provider, plan, coverage area and features that meet the requirements of their job
- Maintain an active service contract for the duration of the stipend;
- Report any cell phone number or plan changes, as well as the loss or theft of a phone within 24 hours.
- Comply with all Federal and State data maintenance and protection laws (e.g., Family Educational Rights and Privacy Act (FERPA), records retention requirements), as well as all Citadel policies, including those pertaining to data security, acceptable computing use, email, etc.;
- Delete all Citadel data from the cell phone when employment with the College is severed, except when required to maintain the data in compliance with a litigation hold notice;
- Will not download or transfer sensitive business data to an employee-owned device; this excludes Citadel email which is protected through the various security controls listed below;
- Will protect the device with a password or other form of user authentication;
- User agrees to maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer; the user will not "jail break" the device by installing software that allows the user to bypass standard built-in security features and controls;
- User agrees that the device will not be shared with other individuals or family members, due to the business use of the device. (e.g., potential access to government e-mail, sensitive data, etc.);
- User agrees to delete any sensitive business files that may be inadvertently downloaded and stored on the device through the process of viewing email attachments; and
- Upon request by The Citadel, the user must allow the installation of mobile device management software or any other software deemed necessary, on the user's device.

Employee Certification.

I certify that I have read, understand, and agree to the Mobile Device Distribution and Use Policy and my responsibilities under the policy. I further certify that the above stipend will be used toward expenses that I incur for mobile device usage for business purposes. I understand that The Citadel is not responsible for the business use of my personal cellular device.

_____ _____

Employee Signature *Date*

_____ _____

Department Head Signature *Date*

Annex B
The Citadel Mobile Device Stipend Allowance Guidance

1. Basic Phone Eligibility.

   A. The job function of the employee requires considerable time outside of his/her assigned office or work area and it is important to The Citadel that s/he be accessible during those times.

   B. The job function of the employee requires him/her to be accessible outside of scheduled or normal working hours or in times of crisis.

Criteria	Stipend Amount
A **and** B above	$40.00/month
A **or** B above	$20.00/month

2. MiFi/iPad Eligibility.

   A. The job function of the employee requires him/her to have wireless data and internet access outside of scheduled or normal working hours or in times of crisis **on a device larger or with more capabilities than a smartphone**.

Criteria	Stipend Amount
A	$10.00/month

3. Smartphone Eligibility.

   A. The job function of the employee requires considerable time outside of his/her assigned office or work area and it is important to The Citadel that s/he be accessible during those times.

   B. The job function of the employee requires him/her to be accessible outside of scheduled or normal working hours or in times of crisis.

   C. The job function of the employee requires him/her to have wireless data and internet access outside of scheduled or normal working hours or in times of crisis.

Criteria	Stipend Amount
All of the above	$60.00/month
C **and** (A **or** B)	$30.00/month