23830 Procedure - Mobile Communication Device

Allowance Calculation

Under the principle that the university should provide employees with the tools necessary to perform their jobs, the university has two options for the provisioning of mobile communication devices and service plans. The purpose of this document is to provide guidance and procedures for the effective implementation of the Allowance Payment Option, Option #2 in Policy 3960**.** This option should be selected only when mutually agreed upon between the department head and the employee. Option #2 is not intended to be used to inappropriately burden the employee or as a means of cost reduction for the department. Employees who have been issued a university-provided device and service plan and wish to change to Option #2 and receive a reimbursement allowance must gain approval from their Department Head. Departments must remember to notify CNS and cancel the existing university plan to terminate the associated charges. Option #2 is limited to salaried employees.

The allowance is calculated as 50 percent of the current market cost (rounded) for a typical device and service plan with one of the major service providers. The department head will determine if the employee requires Voice/Text or a Voice/Text plus Data package.

The allowance amount for Voice/Text reflects 50 percent of the current average market price for Verizon, AT&T, and Sprint calling plans and a basic mobile communication device. These particular plans include unlimited minutes and text. The employee is not required to use one of these vendors. The employee may select a provider as desired provided the services meet the business requirements of the department.

The allowance amount for Voice/Text/Data reflects 50 percent of the current average market price for the Verizon, AT&T, and Sprint Large Data Plan with unlimited Talk / Text, and a Smart Phone. This plan includes 6 GB of Data. The employee is not required to use one of these vendors. The employee may select a provider as desired provided the services meet the business requirements of the department.

The below allowances have been calculated based on 50 percent of the current market cost (rounded) to reimburse the employee for the business usage of a personal device and service plan. The service device amount reflects 1/24 of the total costs of a device which is the current industry standard for amortizing the cost of this technology in consumer plans. Please note, the amounts in the table below are the **monthly** disbursement amount (effective 12/25/17) and not per paycheck:

Coverage Needed	Plan Charges	Line Access Charges	Device Charges	Taxes and Surcharges	Monthly Plan Cost	Monthly Allowance Amount
Voice/Text	$5.00	$20.00	$4.00 (1/24 of $96)	$4.00	$33.00	**$17.00**
Voice/Text/Data (6GB)	$60.00	$20.00	$29.00 (1/24 of $700)	$6.00	$115.00	**$58.00**

Allowance Procedures

- To qualify for an allowance, the employee must meet one of the eligibility requirements outlined in section 2.1 of the university's mobile communication device policy. After the department head determines the employee meets at least one of the eligibility requirements and the allowance option is mutually agreed upon, the employee is responsible for obtaining a mobile communication device and monthly service plan that meets or exceeds the level of service required to fulfill job responsibilities. Note: federal grants and/or sponsored projects do not permit paying allowances for a Mobile Communication Device (MCD) due to the inability to assign costs with accuracy and efficiency (OMB Circular A-21 Section D.1).
- Allowances apply only to employee-owned MCDs and must be less than the employee's monthly cost to maintain the device. An allowance will be paid to the employee each pay period through university Payroll as a non-taxable reimbursement for the business use of a personal device and monthly service plan. The reimbursement for the business use of a personal device has been designated by the Internal Revenue Service as non-taxable if the required documentation and substantiation of business need is met as discussed in the policy and below.
- Employees who have been issued a university-provided device and service plan and wish to change to option 2 and receive a reimbursement allowance must gain approval from their Department Head. Departments must remember to notify CNS and cancel the existing university plan to terminate the associated charges. Note: before allowing an employee to terminate an existing university plan, department heads should consider the cost of device(s) paid for by the department.
- Initial approval (when started) and annual recertification of the business need for the allowance is required and must be documented by December 24 each year using the Mobile Communications Device Request Form. **Without annual recertification, the allowance will automatically terminate on December 24 of each year**. Employees and Departments are encouraged to begin the recertification process in November or early December. The allowance will become effective on the most reasonable processing date after the form is received. **No retroactive payments will be permitted to employees**.
- To obtain an initial allowance or to recertify to maintain an existing allowance:
    - Employees must complete the MCD Request Form, attach a current monthly billing statement from the service provider, sign the form, and obtain the department head's signature. The monthly billing statement must be current (within the last month or two) and the monthly cost of the employee-owned device must be documented. The MCD allowance request cannot exceed the employee's monthly cost for the service on the device used for university business.
    - Departments must complete a P3A-S or P3A-F form and submit it to Human Resources. **All MCD Request Forms should be maintained in the department files**
- The allowance will be reflected on the existing Banner employee job record using a mobile allowance, MA suffix. MA job records have an annual rate (equal to the monthly allowance multiplied by 12). Departments can process a PAF in Banner to manage funding for the MCD allowance (which can be different than funding on the regular position). If the payment is issued and the funding for the allowance needs to be changed retroactively, this can be accomplished using the Labor Redistribution process.
- Employees will see an earn code with a description of MCA on the pay stub. If an employee changes jobs or their job is terminated the allowance will automatically terminate.
- The university will not purchase, repair, or replace the mobile communication device and/or accessories for employees receiving an allowance.
- Employees electing to change from a university provided device to the allowance option should be aware that CNS will not be able to port a business phone number to a personal device. However, CNS does offer

a Unified Communications Mobility package designed to ease the transition. Additional information is available at http://www.nis.vt.edu/uc/support/mobility. These features include:

1. Extend Call - while on an active call on your desk phone, Extend Call allows you to move that call to your cell phone and seamlessly continue your conversation as though you were still on the university telephone network.
2. Mobility (also called EC500) - The Mobility feature is an expanded version of Extend Call. With Mobility activated on your desk phone, all incoming calls will ring to both your desk phone and your cell phone. Either device can answer the call and appear as your Virginia Tech extension to the outside caller.
3. Voice Mail Text Notification- Receive a text message on your cell phone when you receive a voice mail at your university extension.

- Employees are responsible for the protection and retention of university data stored on the device. The portion of data related to business use may be subject to FOIA and/or other appropriate legal requests and the device must be available upon request for such information. Note: Personal information stored on the device, while not typically part of a FOIA request, may be examined by Virginia Tech Information Technology and/or other university personnel during the normal course of compliance with such requests.
- Transmission of Personally Identifiable Information from mobile devices must be encrypted based on The Standard for Storing and Transmitting Personally Identifiable Information.
- Employees receiving an allowance must notify their respective dean, director or department head when mobile communication services are altered or terminated. **The allowance amount must always be less than the employee's monthly cost to maintain the device.**
- *Most Android and Apple iOS phones* provide a way for users to limit or restrict the use of cellular data. Refer to your phone manual for specific instructions. Additionally, the FCC has actively engaged the major cellular service providers to develop an agreement for proactively alerting consumers when they approach usage thresholds that may result in overage charges on their account. Additional information regarding the FCC's involvement in this area can be found at: http://www.fcc.gov/bill-shock-alerts\
- Employees who are eligible to receive a MCD or an allowance and who frequently travel internationally are advised to select option #1 and obtain a university-provided device and service plan. Under option #1, CNS is available to advise employees regarding international travel. Employees who have chosen option #2 and infrequently travel internationally are advised to contact their service plan provider for guidance prior to travelling outside the U.S. Reimbursement for additional charges for international travel is available through the normal travel reimbursement processes with proper supporting documentation, such as a receipt or monthly phone bill with the additional charges displayed.

Mobile Communication Device (MCD) Best Practices

The purpose of these best practice guidelines is to make university employees aware of the potential information security vulnerabilities associated with the utilization of an MCD. All employees who utilize a mobile communication device to conduct university business are advised to read and apply the below security procedures.

General Security

- Keep mobile devices with you at all times or store them in a secured location when not in use. Do not leave your mobile devices unattended in public locations (e.g. airport lounges, meeting rooms, restaurants, etc.).
- Mobile devices should be password protected and auto lockout should be enabled. The password should block all access to the device until a valid password in enabled. The password used should be as strong a password as your device will support.
- Enable a "remote swipe" feature if available. This also includes features that delete data stored on the mobile device if a password is incorrectly entered a certain number of specified tries.
- Do not circumvent security features or otherwise "jailbreak" your mobile device.
- Standard security protocols should be followed. This includes ensuring your device has current anti-virus software and all operating system and application updates and patches. Firewalls should be enabled if possible.
- Wipe or securely delete data from your mobile device before you dispose of it.
- Wipe or securely delete university data from your mobile device when terminating employment with the university.

Transmission Security

- Transmission of Personally Identifiable Information from mobile devices must be encrypted based on The Standard for Storing and Transmitting Personally Identifiable Information.
- Wireless access, such as Bluetooth, WiFi, etc., to the mobile device should be disabled when not in use to prevent unauthorized wireless access to the device.
    - In general, keep your wireless connection on hidden mode unless you specifically need to be visible to others.
- If available, wireless access should be configured to query the user for confirmation before connecting to wireless networks.
    - For example, when Bluetooth is on, select the "check with me before connecting" option to prevent automatic connections with other devices.
- Be careful when using unsecure networks and always use the VT-Wireless or eduroam network to connect while on campus or Virginia Tech's VPN when available remotely.
    - VPN service allows you to access Blacksburg campus university services as though you were on the Virginia Tech network, even though you may be miles or continents away. Limiting service to university network addresses restricts the scope of exposure. For those university services that restrict access to campus network addresses, the remote access - VPN service is a way of selectively re-opening services only to known members of the university community. The remote access - VPN service only encrypts the information between the VPN client and the Virginia Tech VPN gateway. It does not provide end-to-end encryption.

- *The service supports smart phones running the Android and Apple iOS mobile operating systems.* Additional information is available at https://computing.vt.edu/content/virtual-private-network

Application and Data Security

- Do not install software from unknown sources as they may include software harmful to your device. Research any software you intend to install to make sure that it is legitimate.
- When installing software, review the application permissions. Modern applications may share more information about you than you are comfortable with, including allowing for real time tracking of your location.
- Be careful when storing business and personal data on your mobile device. If the device is lost or stolen then the data is also at risk. **Lost, stolen, or misplaced mobile devices should be immediately reported to the Virginia Tech Police. If your mobile device contained university data, also inform your department about a lost, stolen, or misplaced device.** The department head or designee should consider contacting the IT Security Office for further guidance.