Directive   AMS 3300.2   2/14/2013

GUIDANCE ON USE OF MOBILE TECHNOLOGY DEVICES

1.   PURPOSE

This Directive establishes the AMS policy on the purchase, configuration, and use of mobile devices, including smartphones, iPads, iPhones, and tablet computers.

2.   POLICY

End-user mobile technology devices, including laptops, tablets, and smart cellular phones, should be used whenever possible to cost-effectively improve end-user productivity and the customer experience with AMS programs. AMS managers are to evaluate the efficiency of assigning mobile devices to end-users and purchase and assign only the minimal number of appropriately configured devices necessary to accomplish this goal. Government data, including email, must be stored only on Government systems and never on personal, non-Government systems.

3.   MOBILE DATA SECURITY

a.   Storage of Government Data Restricted to Government-Owned or -Managed Devices. All Government data, including email, business notes, and calendar information, will not be copied to non-Government-owned data drives, personally-owned devices that do not have Government mobile device management software installed, or commercial Web storage services such as the Apple iCloud or to non-Government-owned storage devices. When configuring Government accounts, automatic archiving of data to commercial cloud storage services must be disabled.

b.   Government Email Restricted to Government-Managed Email Systems. Government emails will not be copied to personal, non-Government email accounts. Government emails must reside only in Government-managed email systems to protect information from unauthorized disclosure and to meet the Government's legal responsibilities regarding records management. Similarly, Government email archive files (Outlook files with a PST file extension) may not be copied to non-Government owned data drives or Web storage services.

c.   Use of VPN Required When Using Public Wi-Fi Services. To protect Government data in transit across the Internet, after connecting a mobile laptop computer to a public Wi-Fi service, always immediately use the Virtual Private Network (VPN) service to connect to the AMS network. The VPN service will encrypt all data moving across the Internet between the mobile device and the AMS gateway server. For additional security in public locations, also turn off your computer's Bluetooth service.

Smartphones and cellular tablets have data encryption built into their default connections so no special action by the user is necessary.

4. **MOBILE APPLICATION ACQUISITION MANAGEMENT**

   a. Government-Owned Mobile Devices Require Government Application Accounts. A separate Government account/Apple ID must be established by each user and associated with his/her Government-owned mobile devices that use application store accounts (e.g., the App Store or BlackBerry App World). Personal Apple ID or Blackberry accounts may not be used to manage Government-owned devices.

   b. No Default Assignment of Government Credit Cards to Application Store Accounts. When configuring Government accounts, create the account without the association of a credit card. Government credit cards are not to be used as the default billable source for an Apple or BlackBerry application account.

5. **WINDOWS LAPTOP AND TABLET ACQUISITION GUIDANCE**

   a. Prudent Assignment of Mobile Technology Devices.

      (1) One Workstation Device per Employee. AMS managers will typically assign only one workstation device to each employee. Managers will assign a laptop or tablet computer to employees that require a fully functional mobile workstation device. A dockable laptop computer is often the best choice for meeting the in-office and mobile computing needs of AMS users. When a dockable laptop or Windows tablet computer is assigned to an employee, the purchase and assignment of a desktop computer to that same employee is not authorized. Exceptions to this policy will be approved, in writing, by the Deputy Administrator or the Associate Administrator. The assignment of a mobile cellular phone is permitted in addition to the use of a workstation computer.

      (2) Travel Laptop for Office Use. A single laptop can be shared by all travelers in an office, as long as the travel laptop is maintained in a healthy state with current patches and anti-virus signature files.

   b. Optimal Use of Windows Tablet Computers. AMS users are permitted to request the use of a Windows tablet computer in place of a laptop computer. The migration to a Windows tablet device will be part of the regular equipment refreshment cycle for that user.

6. **SMARTPHONE ACQUISITION AND CONFIGURATION GUIDANCE**

   a. Acquisition of Smartphone Devices. AMS users authorized to use a Government-provided smartphone are permitted to choose to use either a RIM BlackBerry smartphone or an Apple iPhone. Users currently using a BlackBerry phone may migrate to an iPhone only as part of the regular upgrade process for existing contracts. Upgrades from an existing iPhone model to a newer iPhone model also are allowed only as part of the regular upgrade cycle for existing contracts. Because of support limitations, the purchase and use of Android phones is not authorized at this time.

b.   <u>iPhone Device Configuration</u>. The most current iPhone model with 16 GB of memory is the default model approved for use by AMS users. Purchases of phones with larger memory must be justified through a waiver provided by the Agency Chief Information Officer (CIO).

c.   <u>Acquisition of Smartphone Applications.</u> BlackBerry and iPhone models will be configured to allow users to download applications from an application store. Personal-use applications that are appropriate for use on Government-owned equipment (e.g., those not related to gambling or pornography) can be downloaded, provided they do not interfere with the performance of official duties. Any personal-use applications that are not free must be purchased with personal funds.

7. APPLE iPAD ACQUISITION AND CONFIGURATION GUIDANCE

a.   <u>Acquisition of iPad Devices</u>. The iPad will be offered to a niche set of users in AMS that need convenient and frequent mobile access to AMS email and Internet news. Deputy Administrators and the Associate Administrator will designate which users are eligible for iPad devices in each Program in consultation with the Agency CIO. The Associate Administrator will designate eligible users for the Office of the Administrator and Staffs.

b.   <u>Acquisition of iPad Applications</u>. iPad users will have access to AMS email and the Internet for Web browsing. Personal-use mobile applications that are appropriate for use on Government-owned equipment (e.g., those not related to gambling or pornography) may be downloaded to the iPad, provided they do not interfere with the performance of official duties. Any personal-use mobile application that is not free must be purchased with personal funds. The cost of mobile applications authorized in advance by a manager for the performance of official duties may be reimbursed by the Agency to the employee as a local expense provided that the reimbursement is appropriately documented (i.e., receipts noting the name of the application, the name of the authorized user, the period of use, and the business justification). End-user support may not be available for mobile iPad applications downloaded for business use.

c.   <u>iPad Device Configuration</u>. Users will need ubiquitous connectivity so the default model will be the Wi-Fi with Cellular using 16 GBs of memory. These devices must be purchased with an annual wireless carrier contract through the Agency's telecommunications acquisition process. Requests for Wi-Fi only iPad models require justification and will use the same technical approval process as laptop or tablet computers. The life cycle of the iPad is considered to be 2 years. After 2 years, a new iPad can be purchased with the Deputy Administrator's or the Associate Administrator's permission.

8. MOBILE DEVICE USE IN LIVESTOCK, POULTRY AND SEED PROGRAMS

For bargaining unit employees in the Livestock, Poultry, and Seed Programs, when the employer determines the employee is in non-pay status, the employee will not be required to perform any job duties using the mobile device, cell phone, iPad, tablet, or laptop assigned by the employer.

9. **INQUIRIES**

    a.   For more information about the use of mobile technology in AMS, contact the office of the AMS CIO at 202-720-1234.

    b.   This Directive is available online at http://www.ams.usda.gov/amsissuances

/s/
Douglas C. Bailey
Chief Information Officer