I POLICY

Resulting from employing mobile computing devices for County business purposes, DoIT shall implement processes and security controls commensurate with the information security risks introduced by the use of mobile devices. This policy hereby incorporates all other applicable County policies, including but not limited to Policies 4.23 and 4.24.

II PURPOSE

The purpose of the Mobile Device Management Policy is to establish the administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for County business purposes.

III KEY TERMS

A. **Laptop Computer** – A portable computer, small enough to rest on the user's lap and having a screen that closes over the keyboard like a lid. Unlike a mobile device, a laptop computer has a computer operating system, and often more robust data storage and peripheral connection capabilities.

B. **Mobile Device** – For the purposes of this Policy, a mobile device is defined as any smartphone or tablet device that transmits, stores, and receives data, text, and/or voice with a connection to a wireless LAN and/or cellular network.

C. **Nonpublic information** – Is information that an employee obtains, or is provided access to, during his/her employment with the County of Cumberland that the employee knows, or reasonably should know, has not been made available to the public. It includes information that the employee knows, or reasonably should know:

   1. Is designated by the County or the Department for which the employee works as nonpublic information;
   2. Contains markings such as “Confidential”, “Internal”, “Restricted”, or similar language, or is considered sensitive information;
   3. Contains information that must be protected by State or Federal Statute, State or County policy, or other regulation;
   4. Is provided to the County for which the employee works by customers or third parties under agreement and with the understanding that it will be treated as confidential, nonpublic information; or
   5. Contains information related to the internal County or Department capabilities and operations that is not available to the public, or that an individual could use to negotiate or otherwise circumvent security controls.

D. **Sensitive information** – Is a term to describe any information which requires protection from unauthorized access or disclosure.

E. **Smartphone** – A handheld mobile communication device with a mobile operating system and an integrated mobile broadband cellular network and Wi-Fi connection capability used for voice and data communications.

F. **Tablet** – An open-faced handheld mobile communication and computing device with a mobile operating system, a touchscreen display, and an integrated Wi-Fi network capability. In some cases, tablets include cellular network connection capability. Tablets resemble smartphones with the major differences being that tablets are not typically used for voice communications and they are larger.

G. **Portable Storage Device** – An information system component that can be inserted into and removed from an information system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks, compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain non-volatile memory).

IV AUTHORIZATION FOR USE OF MOBILE DEVICES

A. DoIT shall review and authorize the use of mobile devices for County business purposes consistent with our internal policies, procedures, applicable State and Federal laws and regulations.
   1. Business Requirement: Mobile devices are provided for official County business use and may be made available or authorized for employees in positions where the associated benefits justify the additional operating costs and/or risks; and
   2. Discretionary Approval: Approval for either providing a user with a County-owned mobile device or allowing the use of a personally owned device for County business purposes, is at the discretion of the CISO; and
   3. Each employee who is issued a mobile device and declared as an "essential employee," will be required to answer or respond when called upon either during or after work hours for notification purposes.

V RISK ASSESSMENT

A. Prior to deploying or authorizing the use of mobile devices for County business purposes, departments must consider the risks associated with the use of mobile devices and establish processes and controls to mitigate them to acceptable levels.
B. Some of the threats introduced by mobile devices include:
   1. Theft/loss of device;
   2. Untrusted/Unsecure wireless networks;
   3. Phishing (email), Vishing (voice), Smishing (text messages);
   4. Rogue apps and malware:
      a) Mobile pick-pocketing: rogue apps may access mobile device resources and carry out fraudulent activities such as the generation of premium text messages (i.e. short message services (SMS)) and premium phone-calls without user intervention or approval;
      b) Stealing of personal information: theft of information like contacts, SMS and media files is widespread, especially on open platforms. A huge market exists for such databases;
      c) Spyware: Smartphones have features like cameras, microphones and GPS tracking.
      d) Several apps allow these features to be activated remotely without the user's knowledge.
C. Prior to leaving the State for traveling purposes, the user of the mobile device must place a Help Desk Ticket to notify DoIT. This will be done to ensure that the account for the device is properly adjusted for billing purposes. This must be done at least five (5) days in advance. It is the mobile devise user's responsibility to place the Help Desk Ticket. If the Mobile Device user fails to do so, then any costs incurred will be at the expense of the Mobile Device user. The decision to allow a user to travel with a County mobile device is at the discretion of the Department Head.

VI NETWORK ACCESS

A. It is understood to consider all personally owned and third-party owned network-capable mobile devices as untrusted and unsecure. Only County-owned and managed mobile devices shall be trusted and permitted to connect to internal agency networks and systems.

B. DoIT may implement guest wireless networks that are segmented from the agency's internal networks to provide network access for personally owned and third-party owned network capable mobile devices. Departments should ensure that users are aware of the prohibition against connecting personal devices to the internal agency networks and consider the use of 802.1X or other Network Access Control (NAC) strategies to enforce network security.

VII TECHNICAL SECURITY CONTROLS

A. DoIT shall ensure the following technical security controls are implemented and enforced on all mobile devices used for County business purposes.

1. Authentication - Logical access to the mobile devices and/or mobile applications that access agency data shall be controlled through the use of authenticators (passwords, biometrics, etc.);
2. Auto-wipe - Where technically feasible, it is suggested that a mobile device shall automatically wipe its contents after 10 consecutive failed login attempts;
3. Session Lock - Mobile devices are required to implement an inactivity locking mechanism to lock the device, and require re-authentication, after no more than five (5) minutes of inactivity;
4. Jailbreaking/Rooting - DoIT shall enforce security controls, and the detection and prevention of their circumvention, through the use of the centralized mobile device management system. Mobile devices that have been jailbroken/rooted shall be denied access to County information assets;
   (The terms jailbreaking and rooting are commonly referred to as the modification of a smartphone or other electronic device to remove restrictions imposed by the manufacturer or operator (e.g. to allow the installation of unauthorized software). Jailbreaking or rooting mobile devices used for County business purposes is prohibited)
5. Anti-Malware - Anti-malware software shall be implemented on all mobile devices, where supported.
6. Operating System Security - where technically feasible, all mobile devices shall have the latest available operating system updates installed upon general release by the device or operating system manufacturer:
   a) Operating system updates/upgrades for County-owned devices as part of their change management processes, are to be administered as needed to ensure security;
   b) Mobile devices used for County business purposes shall allow for remote validation to download the latest security patches by DoIT; and
   c) All mobile devices used for County business purposes shall have the latest available security-related patches installed upon general release by the device manufacturer or carrier.

VIII INVENTORY

A. DoIT shall:
   1. Maintain an inventory of all permitted mobile devices and mobile applications that are used for County business purposes; and
   2. Record all changes to the status of these devices in the inventory.

IX APPLICATIONS

A. DoIT shall:

   1. Approve applications that may be installed and used on mobile devices that are used for County business purposes;
   2. Establish an application validation process to test for device, operating system, and application compatibility issues; and
   3. Non-approved applications shall be prohibited from being installed on County-owned mobile devices or used for County business purposes, regardless of the ownership of the device.
   4. DoIT will vet and ensure that approved applications do not introduce additional risks to the confidentiality, integrity, availability, and privacy of agency data or compromise the security of the device.

B. Any questions regarding if an application is approved should be directed to DoIT through a Help Desk Ticket;

X BACKUP

A. DoIT shall:

   1. Establish mechanisms and requirements to backup mobile devices in order to mitigate the risk of loss of agency information; and
   2. Prohibit the backing up of agency information to personal computers, personal storage devices, and unapproved cloud services.

XI SAFETY AND COMPLIANCE

A. All usage of mobile devices must comply with State, Federal, and local laws in which the mobile device is operated.

XII TRAINING OF MOBILE DEVICE USERS

A. DoIT shall ensure that managers, supervisors, and mobile device users receive security training, addressing at a minimum, the following subjects:
   1. The requirements as outlined herein;
   2. Compliance with legal, regulatory, and contractual requirements related to the use of mobile devices;
   3. The safe use of a mobile device, especially while driving;
   4. The potential risks to the agency's information assets;
   5. Anti-malware awareness training, specific to mobile devices;
   6. The potential risks associated with the use of personally owned mobile devices and the agency's limitations to support personally owned mobile devices;
   7. The use of approved application stores and applications;
   8. Protection of authenticators, such as passwords, personal identification numbers (PIN), and hardware tokens;
   9. The consequences for disabling, altering or circumventing the security configurations that protect agency information assets; and
   10. Security incident management and loss/theft of mobile device reporting procedures.

XIII REFERENCES

A. The requirements established in the Mobile Device Management Policy have been derived from the following:
   1. National Institute of Standards and Technology (NIST) SP 800-53 Access Control (AC), Media Protection (MP), Physical and Environmental Protection (PE); and
   2. NIST CSF Identify/Asset Management (ID.AM), Protect/Access Control (PR.AC), Protect/Information Security Policies and Procedures (PR-IP).