Document Title:	**Mobile Device Acceptable Use and Management Policy**[1] [2]
Document Type:	*Policy*
Document Purpose:	This document establishes the Government technology policy for the use of Government-issued or personal Mobile Devices that access Government servers, data resources, email systems, software and technology infrastructure ("Government systems") or to process or store Government data and information when conducting Government business ("government data"). All users of the Government's technology will ensure the confidentiality, integrity and availability of data provided to, and generated by, Government agencies. This policy exists to prevent data from being deliberately or inadvertently stored or accessed on a mobile device without appropriate security measures; transported over network where the Government data it is at risk and to govern Government issued or owned mobile devices (defined below).
Scope of Application:	This policy applies to all Government Mobile Device users, including employees, authorized contractors, consultants, constitutional employees and temporary employees ("Users").

1. Definition(s)

"Mobile Device" or "Mobile Devices" in this policy refers to all Government-issued mobile devices and personal mobile devices used for Government business. Examples of Mobile Devices include, but are not limited to, smartphones, tablets, notebooks, laptops, Air Cards, netbooks, iPhones and iPads.

[1] This policy template is based on policies provided by Arlington County as a response to the call, by the Mason - NSF project (No. 1623653), for cybersecurity partnership and information sharing among cities and counties.

[2] As used in this document, (i) "Government" means XXX County/City Government, (ii) "CIO" means Chief Information Officer or his/her designee, (iii) "Department of Technology and Information Services" or "DTS" refers to the department that manages the Information Communication Technology, (iv) "CISO" means the Chief Information Security Officer or his/her designee, (v) "Communications Office" refers to the department or designee that manages communications and public relations, (vi) "Chief Records Management Officer" or CRO means the officer that manages Government records policies and enforcement.

2. Issuance and Ownership

(1) A Government-issued Mobile Device may be provided to Users based upon business need and as approved by the department director where the User is assigned.

(2) The purchase and provision of Mobile Devices, accessories and/or services are handled through a Government-wide contract and otherwise must follow Government procurement processes, including prior approval by the appropriate Government personnel. Any exceptions to the Government's standard service and device offerings must be pre-approved in writing by the Chief Information Officer or designee.

(3) Based upon business need, and with department director approval, Users may use personally owned Mobile Devices to access Government systems, to sync email, calendar and contacts etc. Employees using personal devices for Government business are subject to the same usage, security and records management requirements as employees using Government-issued devices.

(4) All Users provided a Government-issued Mobile Device or who use a personal Mobile Device for Government business must comply with the requirements set forth in this policy as well as other related regulations, i.e. *Electronic Communications and Internet Services*[3].

(5) Government-issued Mobile Devices are the property of the Government. All government data stored on a Mobile Device remains the property of the Government and must be handled appropriately.

(6) The physical integrity and security of the Mobile Device is the responsibility of the User to whom the Mobile Device has been assigned or in the owner of a personal Mobile Device.

   a. All Mobile Devices used for Government business must be registered with DTS Help Desk support.
   b. Mobile Devices should be kept in the User's physical presence whenever possible and shall be stored in a secure location at all times (car seats or unlocked glove compartments are not secure storage areas) and away from environment hazards such as heat, water, and chemicals.
   c. The Mobile Device must be protected from unauthorized access and have encryption features activated.
   d. Installation of Mobile Device Management (MDM) software will be required on Government-issued and personal Mobile Devices before access to Government systems will be permitted.
   e. GPS feature full-time activation is required to assist in locating lost or stolen Mobile Devices.

(7) If a Mobile Device is lost or stolen, the incident must be reported to the Help Desk call center as soon as possible, but no later than 24 hours after the loss or theft is discovered. Mobile

[3] Refer to Document VA-01 of Mason - NSF City and County Cybersecurity Partnering, Leadership and Governance Series.

Device access to Government systems will then be denied and the government data stored in the Mobile Device will be deleted (via remote wipe) within 24 hours after the incident is reported.

(8) Users should understand that there is no expectation of privacy in the use or content stored on a Government-issued Mobile Device or any reports generated by the use of a Government-issued Mobile Device, such as a billing statement or charge back statement issued to a department. Such information or data may be collected or reviewed following appropriate Government procedures and may be subject to the provisions of the Virginia Freedom of Information Act (FOIA)[4]. Users of personal Mobile Devices do so at their own risk.

3. Mobile Device Use Requirements and Support

All Users of authorized Mobile Devices agree to the terms and conditions of this use policy t each time they gain access to Government systems at login or use a Government-issued Mobile Device DTS Help Desk Support staff will assist employees authorized to sync a Mobile Device, with initial set-up of the sync feature. DTS will ensure encryption is activated on the Mobile device. Additionally, DTS will, at a minimum, apply the following criteria to the Mobile Device:

(1) Enabled password protection
(2) Retention of e-mails will be set for a maximum of 15 days
(3) Device lock-out after 10 failed login attempts
(4) Auto log-out after 5 minutes of inactivity
(5) GPS activation for lost and stolen recovery purposes.

4. User Responsibilities

All Users must adhere to the following requirements:

(1) Set a password to access the Mobile Device. Do not share the password except with authorized Government personnel;
(2) Immediately report a lost or stolen Mobile Device, or compromised password, to the DTS Help Desk;
(3) Provide full cooperation and support to DTS Help Desk personnel if a remote-wipe of a Mobile Device's content is required;
(4) Take proper care of a Government-issued Mobile Device to protect it against damage, loss and voiding of any applicable warranties;
(5) Comply with the Government's Acceptable Use and Driver Safety policies when conducting Government business while using a Mobile Device;
(6) Compliance with any Litigation Hold for any government data stored on the Mobile Device

[4] https://law.lis.virginia.gov/vacodepopularnames/virginia-freedom-of-information-act/

(7) All Government-issued Mobile Devices must be promptly surrendered when requested by appropriate Government personnel and/or upon separation, resignation or retirement from Government service;
(8) All government data must be removed from a personal Mobile Device, with the assistance of DTS, upon separation, resignation or retirement from Government service or completion of a Government contract, as applicable;
(9) As appropriate, refrain from storing confidential or protected government data on the device and comply with any applicable confidentiality or privacy rules related to government data;
(10) Failure to comply with any of the requirements of this policy or the preventable loss or destruction of a Mobile Device may result in disciplinary action;

Users are also prohibited from:
(11) Downloading, fee-based 'service' that will be charged to the Government without prior department authorization. Services include, but are not limited to Internet, ringtones, music, videos and premium texting;
(12) Downloading any application or service, or modifying the operating system of a Mobile Device which would bypass Government-installed or required security measures;
(13) Downloading any application or service, or modifying the operating system of a Mobile Device in a manner that bypasses or circumvents the Government records retention requirements pursuant to the Virginia Public Records Act, Library of Virginia records retention schedules and guidelines [5];
(14) Violating the Government's Acceptable Use policy and other department policies or Government administrative regulations;
(15) Using the camera feature on a Government-issued Mobile Device in any restroom, locker room, Government medical facility or other area considered by the general public to be private;
(16) Non-exempt employees are prohibited from accessing Government systems outside of their assigned work hours unless pre-approved in writing by authorized department personnel.

5. Departmental Responsibilities

Users must be approved prior to enrollment - Each user is limited to a maximum of 'two' mobile devices. The department director may increase the number of managed devices on a case by case basis. The On-Base Wireless Provisioning process will support enrollment of devices. BYOD devices that are damaged, lost or stolen will not be replaced by the Government.

[5] http://www.lva.virginia.gov/agencies/records/retention.asp

Costs associated with initial purchase and monthly charges for a Government-issued Mobile Device are the responsibility of each individual department and subject to a Government-wide contract. Departments are responsible for employee accounts where spending for-fee-based services (e.g. 411, International Calls and texting in excess of employee's monthly plan) are determined to be excessive.

The department will notify DTS at least 30 days in advance that a Mobile Device is being re-assigned to another employee. If the notification is not received or received after 30 days, the service for the Mobile Device may be terminated.

Each department may adopt department specific policies to supplement this policy and/or to ensure enforcement of this policy. Managers and supervisors are responsible for ensuring that Users of Mobile Devices are aware of and comply with this policy.

In the event a Mobile Device/s or service was previously purchased outside of the Government-wide contract, departments are responsible for promptly transitioning those Mobile Device/s and service contract(s) to the Government-wide contract and notifying the Help Desk to register the Mobile Device/s.