Mobile Device Policy
USG Policy 6 (1.40) | Approved by the Executive Director, May 2019

I. Purpose and Applicability

The purpose of this policy is to specify USG's standards for the use and security of mobile devices. This policy applies to all non-public USG data; see USG Data Classification Policy 6 (2.20) as it relates to mobile devices that are capable of storing such data, including, but not limited to, laptops, notebooks, PDAs, smart phones, and USB drives. Since the policy covers the data itself, ownership of the mobile device is irrelevant. This policy covers any mobile device capable of coming into contact with non-public USG data.

The Universities at Shady Grove is hereinafter referred to as "USG" and the Office of Information Technology as "OIT." This policy will be reviewed annually to ensure continual compliance with USM IT Security Standards and other pertinent policies, laws and industry standards.

II. Definitions

A. *Encryption*: the process of encoding data with an algorithm so that it is unintelligible without the key. Used to protect data during transmission or while stored.

B. *Mobile Devices:* a portable device that can be used for certain applications and data storage. Examples are PDAs or Smartphones.

C. *Mobile Storage Media:* a data storage device that utilizes flash memory to store data. Often called a USB drive, flash drive, or thumb drive.

D. *Password*: a sequence of characters that is used to authenticate a user to a file, computer, or network. Also known as a passphrase or passcode.

E. *PDA*: stands for Personal Digital Assistant. A portable device that stores and organizes personal information, such as contact information, calendar, and notes.

F. *Security Incident:* an instance where USG non-public data, or USG system or device has potentially been or has been exposed to or accessed by an un-authorized party.

G. *Smartphone*: a mobile telephone that offers additional applications, such as PDA functions and email.

III. Physical Security

A. By nature, a mobile device is more susceptible to loss or theft than a non-mobile system. USG should carefully consider the physical security of its mobile devices and take appropriate protective measures, including the following:

1. Laptop locks and cables or docking stations should be used to secure laptops when in the office or other fixed locations.
2. Mobile devices should be kept out of sight when not in use and/or properly secured.
3. Care should be given when using or transporting mobile devices in busy areas. USG OIT will evaluate the data that will be stored on mobile devices and consider remote wipe/remote delete technology. This technology allows users or IT administrator to make the data on the mobile device unrecoverable.
4. USG's OIT will continue to monitor the market for standards and physical security products for mobile devices, as it is constantly evolving.

IV. Data Security

If a mobile device is lost or stolen, the data security controls that were implemented on the device will be the last line of defense for protecting USG's non-public data. The following sections specify the USG's requirements for data security as it relates to mobile devices.

A. Laptops

Laptops must require a username and password or biometrics for login unless otherwise approved by OIT Director and/or the Office of the Executive Director. If laptops contain confidential data as defined in USG's Confidential Data Policy 6 (2.00) all confidential data must be secured consistent with said policy.

B. PDAs/Smart Phones

Use of encryption is not required on PDAs/smart phones but it is encouraged if data stored on the device is especially sensitive. PDAs/smart phones must require a password or passcode for login, however, USG OIT encourages the use of additional security measures where possible (i.e. biometrics and Multi-Factor Authentication).

C. Mobile Storage Media

This section covers any USB drive, flash drive, memory stick or other personal data storage media. USG confidential information stored on mobile storage media is expressly prohibited; see USG Confidential Data Policy 6 (2.00).

D. Other Mobile Devices

Unless specifically addressed by this policy, storing USG confidential data on other mobile devices, or connecting such devices to USG systems, is expressly prohibited. Questions or requests for clarification on what is and is not covered should be directed to the USG OIT Director.

V. Connecting to Unsecured Networks

A. Users are permitted to connect USG-provided computers or devices to public or unsecured networks. Users must take appropriate steps using OIT approved methods and tools when remotely accessing non-public USG data and systems. USG confidential data stored on approved mobile devices within this policy must be protected at all times

when accessing a public or unsecured data; see USG Confidential Data Policy 6 (2.00). Examples of unsecured networks would typically, but not always, relate to Internet access, such as access provided from a home network, access provided by a hotel, an open or for-pay wireless hotspot, a convention network, or any other network not under direct control of the USG.

VI. General Guidelines

A. The following guidelines apply to the use of mobile devices:

1. Loss, theft, or other security incident related to a USG-provided mobile device must be reported promptly.
2. Confidential data should not be stored on mobile devices (personal or USG) unless it is absolutely necessary. If confidential data is stored on a mobile device it must be appropriately secured and comply with the USG Confidential Data Policy 6 (2.00).
3. Data stored on mobile devices must be securely disposed of in accordance with the USG Data Classification Policy 6 (2.10).
4. Users are strongly encouraged to maintain all mobile devices with the latest security updates

VII. Audits

A. USG or an agent of USG will conduct annual reviews to ensure policy compliance.

VIII. Enforcement

A. The enforcement of this policy will be carried out by authorized USG OIT personnel designated by the Director of OIT and USG Senior Leadership. Violations may result in disciplinary actions, which may include suspension, restriction, or revocation of access. Where illegal activities or theft of USG property (physical or intellectual) are suspected, USG may report such activities to the state/federal law enforcement authorities.

IX. Revision History

Date	Description	Revised By
06/15/2018	Initial Policy Creation	Russell Schlosburg

X. Related Documents

A. USM IT Security Standards v4
http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf
B. NIST SP 800-88 "*Guidelines for Media Sanitization*"
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819