Salisbury University

Mobile Device Security Policy

1. PURPOSE

The Salisbury University Information Technology (SUIT) department is committed to managing the confidentiality, integrity, and availability of information technology assets and information.

The use of mobile technology offers employees and contractors new options for work performance and environment, including location, but creates security challenges that include protecting the confidential information accessed by mobile devices. As mobile technology continues to advance, the University will update its policies and processes to incorporate better standards and best practices to ensure data is protected from the latest threats.

2. REVISION HISTORY

Date	Version	Approved By:	Policy Update
12/18/2017	1.0	Dr. Dudley-Eshbach	Initial Publication

3. SCOPE

This policy is applicable to all SUIT environments where mobile device solutions, either employee owned or University owned, are utilized. SUIT will ensure risks of data loss or compromise are mitigated in accordance with the requirements described in this policy.

4. BASE POLICY AND COMPLIANCE REFERENCES

SUIT policy framework is based upon federal, state, and industry best practices and standards. Below is a listing of the base policy and compliance references from University System of Maryland (USM), Federal, State, and other organizations. This policy serves as SU's authoritative adaptation of these policies with specific amendments to meet the business and operational needs of the University.

Policy References

- State of Maryland Department of IT - Cybersecurity Policy: http://doit.maryland.gov/Pages/DoIT-Policy-List.aspx

- USM Security Guidelines: http://www.usmd.edu/usm/adminfinance/itcc/USMITSecurityStandards.pdf

5. POLICY

Mobile devices offer opportunities to streamline agency functions and make employees more productive, but, as with any new technology, inherent vulnerabilities and the ease with which adversaries can exploit those vulnerabilities make implementing mobile solutions a significantly risky and challenging endeavor.

5.1 Mobile Device Definition

According to NIST, and for the purposes of this policy, mobile devices, have the following characteristics:

- **Small form factor**, i.e., relatively small size
- At least one wireless network interface, such as WiFi, cellular, or other technology, used to connect to other data networks
- Local built-in storage
- An operating system (OS) that is not a full-functioning desktop or laptop OS (though this may change as technology continues to evolve)
- Applications available from multiple sources, e.g., provided with the mobile device, available through an "app" store, downloaded via web browser or third-party installers These devices are typically described as smartphones/iPhones, tablets/phablets/iPads, smartwatches, and personal data assistants (PDAs), and have one or more of the common, but optional, characteristics listed below:
- One or more wireless personal-area networks, such as Bluetooth or Near-Field
- Communications (NFC), as well as cellular and GPS services
- One or more digital cameras or video recording devices
- Microphone
- Support for removable storage (e.g., micro-SD cards) and can be used as removable storage by another computing device
- Built-in features for synchronizing data with different locations

5.2 Mobile Device Controls

Individuals using mobile devices, either employee owned or University owned, are not permitted to store any Personally Identifiable Information (PII – See *SU Public and Confidential Information Policy*) on the device. Furthermore if the device is accessing PII it is required to adhere to the following controls

- Passcode or other compensating lock screen control
- System storage both internal and removable is encrypted
- Allow SUIT to remotely wipe or erase the device
- Location features enabled to allow location of the device
- Inactivity lock-out timer set.

5.3 Loss reporting and Disposal

Mobile devices are at higher risk of loss or theft than workstations. SUIT requires that staff report loss or theft of an authorized mobile device immediately.

Disposal of University issued mobile devices creates a risk of potential data compromise; therefore SUIT must ensure proper device sanitization to prevent unauthorized data recovery. See *SU Media Protection Policy.*

6. EXEMPTIONS

If an exemption from this policy is required, an SUIT Policy Exemption Form needs to be submitted and it needs to clearly articulate the reason for the exemption. An operational risk assessment will be conducted to identify the risks associated with this exemption. If the University can accept the risk, an exemption to this policy may be granted**.**

7. DEFINITIONS

Term	Definition
Bring Your Own Device (BYOD)	The practice of allowing the employees of an organization to use their own computers, smartphones, or other devices for work purposes.
Small Form Factor	Term used to describe the physical dimensions of a computing device…small form factor being attributed to mobile technologies such as tablets and smartphones due to the smaller size in comparison to desktop and laptop computers.

8. ENFORCEMENT

SUIT is responsible for ensuring the security of mobile devices for the University. Any systems under the policy authority of SUIT with requirements that deviate from the SUIT Security Program policies are required to submit a Policy Exemption Form to SUIT for consideration and potential approval.

Any attempt by personnel to circumvent or otherwise bypass this policy or any supporting policy will be treated as a security violation and subject to investigation. The results of the investigation may entail written reprimand, suspension, termination, and possibly criminal and/or civil penalties.