


**Coppin State University
Information Technology Division
Policies and Procedures**

<u>Policy #:</u>	ITD – CCS – 016	Version: 01
<u>Subject:</u>	CSU Mobile Device Management Policy	Effective Date: 09/01/2013
<u>Approved by:</u>		<u>Approval Date:</u> 12/14/2016
		Review Date: 12/14/2016

I. Purpose

The purpose of this policy is to establish criteria for standardizing and managing CSU issued mobile devices *not including laptops*.

II. Policy

The acquisition, assignment, and use of CSU cellular telephones/smartphones are intended for University business purposes.

III. Procedure

Mobile Device Requirements

Android

- *Require 4-digit pin/password*
- *Remote Data Deletion*
- *Enforce storage card encryption*
- *Enforce file encryption*

iOS

- *Require 4-digit pin/password*
- *Remote Data Deletion*
- *Enforce storage card encryption*
- *Enforce file encryption*

Windows

- *Require 4-digit pin/password*
- *Remote Data Deletion*
- *Enforce storage card encryption*
- *Enforce file encryption*

Mobile Device Management

CSU utilizes management software to ensure CSU issued mobile devices and installed applications meet the BOR Requirements for mobile devices

Management Software App:

Android

- *Allow only policy managed app to transfer data*
- *Allow only policy managed app to cut, copy and paste*
- *Require device compliance with CSU policy for access*

iOS

- *Allow only policy managed app to transfer data*
- *Allow only policy managed app to cut, copy and paste*
- *Require device compliance with CSU policy for access*
- *Encrypt data when locked*

Windows

- *Allow only policy managed app to transfer data*
- *Allow only policy managed app to cut, copy and paste*
- *Require device compliance with CSU policy for access*

CSU employees are accountable to exercise care in the use of University equipment and property and use such property only for authorized CSU purposes. Intentional misuse of University property may be considered grounds for disciplinary action.

Each University Division must establish their own criteria and procedures for approving mobile device services that must comply with CSU policies.

Responsibilities:

Each Division has a responsibility to:

- *Maintain inventory of all mobile devices and services acquired for divisional use.*
- *Ensure that divisional cellular service users comply with all applicable CSU policies.*

- *Ensure PII/Sensitive/Non-public information shall not be collected or stored on mobile devices*
- *Devices are enrolled in the company /CSU portal*
- *Ensure that in case of loss, damage, or theft of equipment, users shall notify the IT Help Desk immediately*

The Employee has a responsibility to:

- *Use mobile devices responsibly and comply with applicable laws and regulations.*
- *Comply with other applicable CSU policies.*
- *Devices are enrolled and remain enrolled in the company /CSU portal*
- *Ensure PII/Sensitive/Non-public information shall not be collected or stored on mobile devices*
- *Ensure that in case of loss, damage, or theft of equipment, users shall notify their division and IT Help Desk immediately.*

All telecommunications service requests shall be submitted to the IT Help Desk

- Phone: (410) 951-3888
- E-Mail: oithelpdesk@coppin.edu

IV. Definitions

The following terms apply for the purpose of this policy. Definitions for these terms may be found at <https://lookup.coppin.edu/cpd/Pages/Home.aspx>:

[Accountability](#)

[Network](#)

[Authorization](#)

[Policy](#)

[Business Need](#)

[Smartphone](#)

V. References

- Policy: ITD-TEL-005, CSU Cellular Telephone/Smartphone Policy
- Policy: ITD-TEL-011, CSU Cellular/Smartphone Disposal Policy
- Policy: ITD-GEN-013, CSU Non-Public Information Policy
- Policy: CSU Student Computer Use and Internet Access Policy
- Policy: CSU Faculty/Staff Computer Use and Internet Access Policy