COMPLIANCE COMPONENT

DEFINITION

Name	Mobile Device Security Management
Description	Mobile device security management is a process that secures mobile devices. Mobile Devices (i.e., smartphones, tablets, etc.) are portable computing devices that have a small form factor such that they can easily be carried by a single individual; are designed to operate without a physical connection (e.g., wirelessly transmit or receive information); possess local, non-removable data storage; and are powered on for extended periods of time with a self-contained power source. Laptops are not considered mobile devices.
Rationale	Ensures that only approved devices have the capability to be connected to an agency network.
Benefits	Properly securing these devices: • Protects the network from malicious activity • Prevents compromise of agency information • Allows users to securely work remotely

ASSOCIATED ARCHITECTURE LEVELS

Specify the Domain Name	Security
Specify the Discipline Name	Technical Controls
Specify the Technology Area Name	Remote Access Controls
Specify the Product Component Name	

COMPLIANCE COMPONENT TYPE

Document the Compliance Component Type	Guideline

Component Sub-type	1. **Enterprise Mobile Device Deployment Life Cycle -** There are many factors to consider when deploying mobile devices within an enterprise environment. These include selecting the correct management technologies and devices, alongside properly providing them to users. a. **Identify Mobile Requirements -** In the first stage of this life cycle, the organization’s decision makers define the mission needs and requirements for mobile devices, inventory the mobile devices already in use, and identify the mobile deployment model that fits their organization. The participation of both IT-focused and business-focused decision makers is necessary at this stage to ensure that the needs of the mission will drive the technology choices in later stages. b. **Perform Risk Assessment -** Risk assessments are a foundational component of cybersecurity. The risk-assessment process can be used to identify, estimate, and prioritize risk to organizational operations and assets, staff, and other organizations that result from the operation and use of information systems. Risk assessments should be performed periodically, as the threat landscape is constantly changing and the systems to be protected are evolving. c. **Implement Enterprise Mobility Strategy -** Resource availability, mission needs, and various other organization constraints will guide decisions on mobile deployment options, devices, and electronic mobility management (EMM) systems. Some organizations must have full control of all components in the enterprise environment, so all mobile equipment must be purchased by the organization and managed by enterprise system administrators through an EMM. d. **Operate and Maintain -** It is necessary to design and implement security controls to protect enterprise systems, as well as enterprise and user data. However, the initial deployment of controls is not sufficient to protect an operational enterprise. In addition, IT audits should be used to periodically evaluate the effectiveness of security controls for protecting the evolving enterprise, identify security issues, and modify or add controls to better protect the system in the future. e. **Dispose of and/or Reuse Device -** Mobile devices may hold sensitive information, such as passwords, account numbers, emails, voicemails, text message logs, or mission-specific data (e.g., sensitive law enforcement information). When a mobile device must be disposed of, it is important to take the proper steps to ensure that sensitive information does not fall into the wrong hands. **2. Agencies should consider the following when securing a mobile device:** • Agencies should purchase and/or approve devices that will be securely managed. • Mobile devices must adhere to all agency policies and guidelines. • Only approved equipment may have access to the state network regardless of the method of access. • Users must be briefed in computer security awareness.

- Users shall exercise due diligence in protecting the device and the network they access from unnecessary risks.
- All devices shall be encrypted.
- Screen lock must be enabled within an agency's specified time period.
- Any device that is lost, stolen, or no longer in the user's possession, shall immediately be reported to the appropriate agency personnel.
- Devices shall be configured to be erased (wiped) remotely in the event it is lost, stolen, no longer in the user's possession or the employee is no longer with the agency.
- Devices should be configured to allow location tracking.
- Devices whose operating system has been modified from the agency-approved settings will not be allowed on the agency network.

This document will be reviewed annually or as needed.

Compliance Detail

State the Guideline, Standard or Legislation	○ Guidelines for Managing the Security of Mobile Devices in the Enterprise.
Document Source Reference #	NIST 800-124, Rev. 2
State the Guideline, Standard or Legislation	State of Missouri Administrative Policy – Personal Mobile Device Security?
Document Source Reference #	

Compliance Sources

Name	National Institute of Standards and Technology (NIST), Computer Security Resource Center (CSRC)	*Website*	http://csrc.nist.gov/
Contact Information	Inquiries@nist.gov		
Name		*Website*	
Contact Information			

Keywords

List Keywords	Cell, ipod, iphone, ipad, smartphone, mobile, phone, encryption, password, device, anti-virus, wiped, operating system, Electronic Mobility Management (EMM).

Component Classification

Provide the Classification	□ *Emerging*	☒ *Current*	□ *Twilight*	□ *Sunset*
Sunset Date				

Component Sub-Classification

Sub-Classification	Date	Additional Sub-Classification Information
□ *Technology Watch*		
□ *Variance*		

□ *Conditional Use*		

Rationale for Component Classification

Document the Rationale for Component Classification	

Migration Strategy

Document the Migration Strategy	

Impact Position Statement

Document the Position Statement on Impact	

Current Status

Provide the Current Status	□ *In Development*	☒ *Under Review*	□ *Approved*	□ *Rejected*

Audit Trail

Creation Date	08-22-2013	*Date Approved / Rejected*	02/13/2025
Reason for Rejection			
Last Date Reviewed	01/28/2025	*Last Date Updated*	02/13/2025
Reason for Update	Vitality		