



State of Illinois
Department of Central Management Services

MOBILE DEVICE SECURITY POLICY

Effective: October 01, 2009

State of Illinois

*Department of Central Management Services
Bureau of Communication and Computer Services*

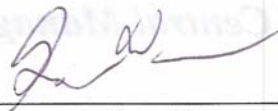
MOBILE DEVICE SECURITY POLICY

Effective October 01, 2009

Version 1.0

APPROVAL SHEET

State CIO



Greg Wass

Date:

9/30/09

CMS Director:

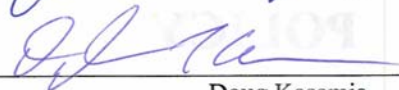


James F. Sledge

Date:

9-9-09

CMS/BCCS Deputy
Director:



Doug Kasamis

Date:

9/08/09

CMS/BCCS Deputy General
Counsel:

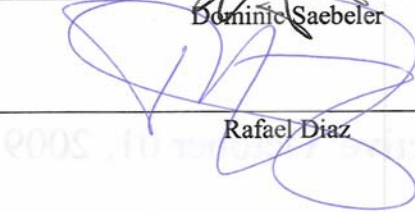


Dominic Saebeler

Date:

9/3/09

CMS/BCCS Chief
Information Security Officer:



Rafael Diaz

Date:

9/02/09

**Please Return to: CMS/BCCS
Chief Information Security Office
120 W. Jefferson
Springfield, IL 62702**

Thank You.

TABLE OF CONTENTS

POLICY STATEMENT

PURPOSE

SCOPE

DEFINITIONS

ENFORCEMENT

RESPONSIBILITY

POLICY

Illinois Department of Central Management Services
MOBILE DEVICE SECURITY POLICY

POLICY STATEMENT

The Illinois Department of Central Management Services, Bureau of Communication and Computer services (CMS/BCCS) seeks to protect State of Illinois (State) mobile devices from unauthorized access, use, disclosure, alteration, modification, deletion, destruction and/or removal.

PURPOSE

This document describes the minimum security policy for State of Illinois mobile devices. Mobile devices must be appropriately secured to prevent sensitive or confidential data from being lost or compromised, to reduce the risk of spreading viruses, and to mitigate other forms of abuse of the State of Illinois' computing and information infrastructure.

SCOPE

This security policy (Mobile Device Security Policy) applies to the user of any State mobile device which connects to the CMS/BCCS managed network / resource.

DEFINITIONS

Definitions for terms used in this policy can be found in the *BCCS Terminology Glossary* located at <http://bccs.illinois.gov> . The terms and definitions listed below are meaningful for this policy. In the event of conflict between the definition in the *BCCS Terminology Glossary* and the definition contained in this policy, the definition below shall control for this Policy.

1. **Mobile Devices:** These include, but are not limited to, Portable Digital Assistants (PDAs), notebook computers, Tablet PCs, Palm Pilots, Microsoft Pocket PCs, RIM Blackberrys, MP3 players, text pagers, smart phones, compact discs, DVD discs, memory sticks, USB drives, floppy discs and other similar devices.
2. **User** - Anyone with authorized access to State business information systems, including permanent and temporary employees or third-party personnel such as temporaries, contractors, consultants, and other parties with valid State access accounts.
3. **Screen Lock** - Mechanism to hide data on a visual display while the computer continues to operate. A screen lock requires authentication to access the data. Screen locks can be activated manually or in response to rules.
4. **Screen Timeout** - Mechanism to turn off a device or end a session when the device has not been used for a specified time period.

ENFORCEMENT

Noncompliance with this policy and/or its resulting procedures may be cause for disciplinary action up to and including discharge, may involve civil or criminal litigation, and may involve restitution, fines, and/or penalties.

RESPONSIBILITY

1. Each user of a State mobile device is responsible for following this policy and any related policy or procedure promulgated by their Agency head.

Illinois Department of Central Management Services
MOBILE DEVICE SECURITY POLICY

2. Each Agency may also establish policies and procedures and assign responsibility to specific agency personnel to achieve compliance with this policy.
3. Anyone observing what appears to be a breach of security, violation of this policy, violation of state or federal law, theft, damage, or any action placing State resources at risk must report the incident to an appropriate level supervisor, manager, or security officer within their organization. Those reporting alleged incidents will be protected from retaliation by existing whistleblower protection laws.
4. Managers and supervisors are responsible for ensuring that users are aware of and understand this policy and all related procedures.

POLICY

1. Whenever possible, all mobile devices must be password protected. Choose and implement a strong password – at least eight (8) characters in length.
2. The physical security of these devices is the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee’s physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.
3. If a mobile device is lost or stolen, promptly report the incident to the CMS/BCCS Help Desk and proper authorities. Also, be sure to document the serial number of your device now, for reporting purposes, in the event that it is lost or stolen.
4. Sensitive or confidential documents, if stored on the device, should be encrypted if possible.
5. Mobile device options and applications that are not in use should be disabled.
6. Sensitive and confidential information should be removed from the mobile device before it is returned, exchanged or disposed.
7. Whenever possible all mobile devices should enable screen locking and screen timeout functions.
8. No personal information (as defined by the personal information protection act – 815 ILCS 530) shall be stored on mobile devices unless it is encrypted and permission is granted from the data owner.
9. Before a mobile device is connected to State IT systems, it shall be scanned for viruses (the user risks having files on the device deleted if any viruses are detected). If media mobile device is used for transitional storage (for example copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.

- End of Mobile Device Security Policy -