State of Iowa Department of Corrections

Policy and Procedures

Policy Number: AD-IS-03
Applicability: Institutions, CBC, Central Office, IPI
Policy Code: Public Access
Iowa Code Reference: N/A
Chapter 1: ADMINSTRATION AND MANAGEMENT
Sub Chapter: INFORMATION SYSTEMS/RESEARCH
Related DOC Policies: N/A
Administrative Code Reference: N/A
Subject: MOBILE DEVICES
PREA Standards: N/A
Responsibility: John Needelman
Effective Date: June 2023
Authority:

1. PURPOSE

To provide guidelines on the use of mobile devices used for Iowa Department of Corrections (IDOC) business.

2. POLICY

This policy applies to all state-owned as well as personal mobile devices used for IDOC business. Mobile devices are defined as any small or portable device capable of making a cellular connection that can be used for data and/or voice communication using an Internet connection.

CONTENTS

3. DEFINITIONS

A. Hotspot - A wireless Ethernet access point connected to a cellular data network that can allow wireless network capable devices, without direct cellular service, to connect to said service.

B. Short Message Service (SMS) – SMS is a form of text messaging communication on mobile phones.

C. SSID - The primary name associated with a Wireless Local Area Network (WLAN).

D. Peer to Peer Messaging (PIN to PIN) – A communication method in which the involved parties send information directly between each other without using a go-between. A situation in which a third party is used to initiate the communication between peers, but is not used to maintain the connection is also considered peer-to-peer.

E. WiFi - name given to networking equipment that presents a WLAN.

F. See IDOC Policy **AD-GA-16** for additional Definitions.

4. PROCEDURES

A. Device settings configured by email server:

1. Passwords/PINs – Passwords/PINs must be enabled for each device. Passwords/PINs must have a minimum length of four characters.

2. Erase Data and Disable Device – The device must have the ability to be remotely erased and disabled:

    a. After 10 unsuccessful password attempts.

    b. When reported lost or stolen.

3. Inactivity – The device must be set to lock after a maximum of 15 minutes of inactivity.

B. Device setting configured by user or System Administrator

1. Confidential information shall not be sent by SMS.

2. Confidential information shall not be sent by peer-to-peer messaging.

3. Security Patches – Software upgrades and security patches must be applied in a timely manner.

4. Third Party Applications – Users may not download third-party applications to their device without prior approval. IDOC reserves the right to review the applications installed on mobile devices. IDOC shall maintain a list of the applications installed on each device.

5. Camera – Use of the camera feature, including video, is prohibited in areas displaying, storing, or transmitting confidential information including health information.

6. Reporting – Users must report lost, stolen, or missing devices to their Duty Officer within 12 hours. The Duty Officer shall notify their local Systems Administrator. The Systems Administrator shall notify the Warden/District Director, IDOC Chief Information Officer, then the OCIO Security Operation Center (SOC). Notification to the OCIO SOC shall take place as soon as possible, but no later than 24 hours, after the device is reported missing.

7. Bluetooth – The following settings are required for devices using Bluetooth:

    a. Disable Discovery Mode

    b. Pairing

        1) Attempts to pair devices require prior management approval, all single purpose Bluetooth hands free calling devices are pre-approved by management.

        2) If prompted to pair with another Bluetooth device the user is to deny all requests and report such information to system administrators.

        3) The Bluetooth auto reconnect to authorized devices should be turned off with the exclusion of hands-free equipment.

        4) Data sent between paired devices must be encrypted.

8. The user and/or the Systems Administrator must ensure that IDOC and personal email and contacts do not become co-mingled in a single storage volume. This must be differentiated from situations where the data is stored separately but displayed co-mingled.

a. Hotspot Usage - There are two typical types of hotspots used. Both need to be secured in a similar manner to limit security risk.

    1) Dedicated - A single purpose hotspot for allowing multiple connections.

    2) The highest level of connections encryption that the hotspot allows shall be enabled.

    3) Cross connection between devices connected to the hotspot shall not be allowed.

    4) The Pre-Shared Key (PSK) used in connecting to the hotspot shall follow complexity rules.

    5) Usage of a hotspot shall be considered the same as a public unsecured network. All connections to Department or State resources shall be over an encrypted or VPN connection.

    6) Automatic connection and reconnection shall not be allowed. All connections shall be individually authorized including reconnections.

    7) On Department owned hotspots only Department owned equipment shall be allowed to connect.

    8) The hotspot shall be running a current supported firmware, and shall not be considered End-of-Life or End-of-Support.

b. Integrated - A general purpose cellular connected device that can also act as a hotspot.

    1) SSID for the network shall not broadcast. Change SSID to remove any reference to the name of the phone or its owner.

    2) The highest level of connection encryption that the hotspot allows shall be enabled.

    3) Cross connection between devices connected to the hotspot shall not be allowed.

    4) The Pre-Share Key (PSK) used in connecting to the hotspot shall follow complexity rules.

5) Usage of a hotspot shall be considered the same as a public unsecured network. All connections to Department or State resources shall be over an encrypted or VPN connection.

6) Automatic connection and reconnection shall not be allowed. All connections shall be individually authorized including reconnections.

7) On Department owned hotspots only Department owned equipment shall be allowed to connect.

8) The hotspot shall be running a current supported firmware, and shall not be considered End-of-Life or End-of-Support.

C. End of Use

1. Devices

   a. Android Based Devices

      Where the device supports use the recovery mode to erase all storage volumes. Otherwise use the available erase mechanisms, and verify data is purged.

   b. Apple IOS Devices

      Use the reset function to erase all content and settings.

   c. Alternate option for End-of-Life devices, using a certified third party have the device destroyed with a certification of destruction.

2. Associated Accounts

   a. When the account associated with the device is no longer needed, any associated cloud based storage shall also be cleared.

   b. With a verification of the data being cleared the account can be destroyed.

D. Non-compliance

Non-compliance to any aspects of the policy may result in removal of mobile access to the enterprise email system, wiping of the mobile device and disciplinary action.

E. Notice

Based on a FIOA request or litigation, up to and including all contents of a device used in conjunction with work duties and/or said device and all data contained within could have to be made available.