Beverly A. H. Buscemi, Ph.D.
State Director
David A. Goodell
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
Thomas P. Waring
Associate State Director
Administration

SOUTH CAROLINA Department OF Disabilities AND Special Needs

3440 Harden Street Ext (29203)
PO Box 4706, Columbia, South Carolina 29240
803/898-9600
Toll Free: 888/DSN-INFO
Website: www.ddsn.sc.gov

COMMISSION
William O. Danielson
Chairman
Eva R. Ravenel
Vice Chairman
Gary C. Lemel
Secretary
Mary Ellen Barnwell
Sam F. Broughton, Ph.D.
Catherine O. Fayssoux
Vicki A. Thompson

Reference Number:	367-15-DD
Title of Document:	Mobile Device Security Policy
Date of Issue:	July 10, 2015
Effective Date:	July 10, 2015
Last Review Date:	July 10, 2015
Date of Last Revision:	July 13, 2016 **(NEW)**
Applicability:	All DDSN Employees

I. PURPOSE

The purpose of this policy is to establish the procedures and requirements necessary to protect the security of DDSN information when accessed from mobile devices, including but not limited to smart phones and tablet computers.

1. This policy includes usage restrictions, configuration management, device authentication, and implementation of mandatory security software.

2. This policy applies to DDSN owned mobile devices or employee owned devices which access DDSN data or the DDSN data network.

II. SECURITY PROCEDURES AND REQUIREMENTS

1. DDSN only allows access by mobile devices which are assigned and identified to an individual owner. Employees who are approved to access DDSN data or the DDSN data network using their personal device must register the device with the DDSN Information Technology Division (IT).

2. DDSN shall utilize mobile device management software to manage all mobile devices which access DDSN data or the DDSN data network. This includes agency owned and employee owned mobile devices.

3. DDSN shall utilize a mobile device management agent which will encrypt DDSN data on mobile devices using industry standard encryption techniques.

4. Employees must allow DDSN IT personnel to install DDSN's mobile device management agent in order to protect the security of DDSN data and the DDSN network.

5. Employees must allow DDSN IT personnel to scan mobile devices for viruses before they access DDSN data or the DDSN network. They must subsequently allow an automated virus scanning process to run on a regular basis without interfering with or aborting the process.

6. DDSN only allows access by mobile devices that have the ability to be remotely wiped / erased by DDSN's MDM software in the event of loss, theft or evidence that DDSN data has been compromised.

7. Any mobile device must be approved by DDSN's designated Information Security Officer before accessing DDSN data or network. Only device types/operating systems that are supported by DDSN's MDM agent will be allowed to access DDSN's network and data.

8. Mobile devices with operating systems that have been modified from the standard provided by the mobile provider will not be allowed to access DDSN data or the DDSN network. "Rooting" and "Jail-breaking" is not allowed on phones which access DDSN data or the DDSN network.

9. Employees must notify DDSN's IT Division before the mobile device is disposed, sold, surrendered to a mobile provider, or otherwise deactivated and allow IT personnel to remove sensitive and confidential information from the mobile device.

10. If a mobile device which has access to DDSN data or the DDSN network becomes lost or stolen, the employee must notify DDSN's IT Division immediately via the Helpdesk phone number or email. DDSN will maintain the technical capability of remotely wiping data from the lost or stolen device and will do so to mitigate risks associated with the lost or stolen mobile device.

11. All mobile devices which have access to DDSN data or the DDSN network must have security activated that requires a password or passcode to unlock the phone and gain access to its data. The timeout/lockout feature must be enabled which requires the password or passcode to be entered to gain access to the device after it has not been used for a period of time.

12. Unencrypted DDSN data shall not be copied to or stored on removable media on mobile devices (SD cards, etc.).

13. Unencrypted DDSN data shall not be copied from the mobile device to external storage media by any means (USB or other wired connectivity, Bluetooth or other wireless technology).

III. MOBILE DEVICE ACCESS AGREEMENT

1. Employees who are approved to have mobile devices which accesses DDSN data or the DDSN network shall sign the DDSN Mobile Device Access Agreement (see attachment) before being granted access.

2. The Mobile Device Access Agreement must also be signed by the manager of the employee requesting access. By doing so, the manager is indicating that the employee has a valid business need to access DDSN data and the DDSN network using a mobile device.

3. By signing the DDSN Mobile Device Access Agreement the employee agrees that the physical security of the device shall be 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.

IV. IMPLEMENTATION, MAINTENANCE, AND COMPLIANCE

1. DDSN's designated Information Security Officer is responsible for insuring that this policy is implemented and communicated throughout DDSN.

2. Any revisions to this policy shall be developed by the designated Information Security Officer and follow the normal approval process according to DDSN Directive 100-02-DD: Implementation Procedures for the Internal Communications System.

3. Violation of the provisions of this directive will be subject to disciplinary action in accordance with DDSN's progressive discipline policy.

Tom Waring
Associate State Director-Administration
(Originator)

Beverly A.H. Buscemi, Ph.D.
State Director
(Approved)

Reference: NIST SP 800-53 Revision 4: Media Use
NIST SP 800-53 Revision 4: AC 19 Access Control for Mobile Devices
NIST SP 800-53 Revision 4: PS 6 Access Agreements

To access any Guidance references, please see the attached link at:
http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

To access the following attachments, please see the agency website page "Attachments to Directives" under this directive number at http://www.ddsn.sc.gov/about/directives-standards/Pages/AttachmentstoDirectives.aspx.

Attachment: Mobile Device Access Agreement