Reference Number:	367-20-DD
Title of Document:	Portable Computing Devices
Date of Issue:	December 10, 2014
~~Late Review Date:~~	~~December 10, 2014~~
Date of Last Revision:	~~July 13, 2016~~XXXX, 2023 (~~NEW~~**REVISED**)
Effective Date:	~~December 10, 2014~~XXXX, 2023
Applicability:	All DDSN Employees

~~I. PURPOSE~~

~~The purpose of the Portable Computing Devices security policy is to establish security mechanisms to protect both portable computing devices, such as laptops, and the information they contain.~~

~~II. Access Control for Mobile Devices~~

- ~~DDSN employs whole disk encryption to protect the confidentiality and integrity of information stored on portable computing devices, including laptops.~~
- ~~DDSN prohibits any passwords to be written or notated on any portable computing devices, including laptops.~~
- ~~DDSN configures portable computing devices operating system so that only approved services are enabled and/or installed by a DDSN information technology (IT) administrator.~~
- ~~DDSN utilizes a configuration management process that includes flaw remediation, installs the most current stable security patches, critical security updates and hot fixes for the relevant operating system.~~

- DDSN utilizes antivirus management tools to automatically update virus definition files on laptops and other portable computing devices susceptible to viruses.
- DDSN installs firewall software on laptops and implements mechanisms that prevent users from making firewall configuration changes.
- DDSN does not allow unauthorized software to be installed on laptops and/or other portable computing devices. Approval shall be obtained for the installation of any software that may be required for business use. A DDSN IT administrator will install any approved software.
- DDSN places asset tags on portable computing devices.
- DDSN does not allow Bluetooth, Infrared, or other wireless technologies to transfer unencrypted data.
- DDSN shall disable Peer-to-Peer wireless connections, otherwise known as "Ad-Hoc Connections," on all portable computing devices, including laptops.
- Employees must notify the DDSN IT Division immediately in the event of a theft or loss using the Helpdesk phone number at 1-803-898-9767 or by email at Helpdesk@ddsn.sc.gov.
- DDSN IT Division shall securely remove Agency data from portable computing devices rendered inoperable or retired.

III. LAPTOP COMPUTER CUSTODY RECEIPT

The Laptop Computer Custody Receipt must be signed by any employee who is issued or returns a permanently assigned laptop. The IT Division maintains a log of short term loaner laptops.

IV. IMPLEMENTATION, MAINTENANCE, AND COMPLIANCE

- DDSN's designated Information Security Officer is responsible for insuring that this policy is implemented and communicated throughout DDSN.
- 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.
- Violation of the provisions of this directive will be subject to disciplinary action in accordance with DDSN's progressive discipline policy.

Tom Waring	Beverly A.H. Buscemi, Ph.D.
Associate State Director-Administration	State Director
(Originator)	(Approved)

Reference: NIST SP 800-53 Revision 4: AC-19 Access Control for Mobile Devices

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

OVERVIEW

Mobile computing devices (smartphones, tablets, laptops, etc.) are becoming an implementation standard in today's computing environment. Their size, portability, and ever- increasing functionality are making the devices desirable in replacing traditional desktop devices. However, the portability offered by these devices can also increase security exposure to individuals using the devices.

PURPOSE

The purpose of this directive is to establish the procedures and protocols for the use of Department of Disabilities and Special Needs (DDSN) mobile devices and their connection to the network.

SCOPE

This directive applies to all DDSN staff who use agency issued mobile computing devices.

GENERAL

All DDSN mobile devices that have access to agency systems and applications are governed by this policy. Applications, including cloud storage software used by staff on their own personal devices are also subject to this policy. The following general procedures and protocols apply to the use of mobile devices:

- Mobile computing devices must be protected with a password or Personal Identification Number (PIN) required at the time the device is powered on.
- Passwords/PINs must meet the requirements outlined in the DDSN Access Control and Password Policy.
- Mobile Device Management (MDM) will be used to enforce security standards and configurations on devices.
- All mobile device physical storage partitions shall be encrypted.
- Wireless encrypted security and access protocols shall be used with all wireless network connections.
- Staff shall refrain from using public or unsecured network connections while using their mobile device.

- Unattended mobile computing devices shall be physically secured.

- Mobile computing devices that access the DDSN network shall have active and up-to-date virus, anti-malware and firewall protection.

- Lost or stolen devices shall have locations services enabled and the units wiped of all information so they are unusable until recovered or destroyed.

MOBILE DEVICE USE

- Mobile communication devices are to be used for official use just as other office equipment, subject only to limited incidental personal use that does not increase the state's cost or violate any laws or ethical standards.

- Employees must reimburse DDSN for any incidental personal use that results in an additional expense to the Department.

- Managers for each Division where these devices are assigned are responsible for collecting any required reimbursement.

- Employees have no expectation of privacy as to the use of a Department issued mobile communication device. Management will have access to detailed records of mobile communication device usage from the service provider, which will be subject to audit.

- Employees who, as part of their official job duties, must use DDSN mobile communication devices while operating a motor vehicle, must follow all South Carolina wireless telecommunication laws (S.248).

USER DEVICE RESPONSIBILITIES

The following procedures and requirements shall be followed by all users of mobile devices:

- Staff must immediately report any lost or stolen devices to the Chief Information Officer or the Chief Information Security Officer.

- Unauthorized access to a mobile device or company data must be immediately reported to the Chief Information Officer or the Chief Information Security Officer.

- Mobile devices shall not be "rooted" or have unauthorized software/firmware installed.

- Staff shall not load illegal content or pirated software onto any DDSN mobile device.

- Only DDSN approved applications are allowed on mobile devices.

- Mobile devices and applications shall be kept up-to-date.

- Operating system and application patches should be installed upon release.

- Personal firewalls will be installed and active where available.

ADMINISTRATIVE RESPONSIBILITIES

- Specific configuration settings shall be defined for personal firewall and malware protection software to ensure that that this software is not alterable by users of mobile devices.

- Mobile Device Management (MDM) software is used to manage risk, limit security issue, and reduce costs and business risks related to mobile devices. The software shall include the ability to inventory, monitor (e.g. application installations), issue alerts (e.g. disabled passwords, categorize system software (operating systems, rooted devices), and issue various reports (e.g. installed applications, carriers).

- MDM software enforces security features such as encryption, password or PIN requirements, remote wiping, inactivity timeouts and key lock on mobile devices.

- MDM software shall include the ability to distribute applications, data, and global configuration settings against groups and categories of devices.

- Regular reviews and updates of security standards and strategies used with mobile computing devices.

- Procedures and policies exist to manage requests for exemptions and deviations from this policy.

ENFORCEMENT

Failure to comply with the mobile device directive may, at full discretion of DDSN, result in the suspension of technology use and connectivity privileges, disciplinary action, and possibly termination of employment.

Barry D. Malphrus
Vice Chairman

Stephanie M. Rawlinson
Chairman