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

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
Fred Lynn
Chairman
Christine Sharp
Vice Chairman
Harvey E. Shiver
Secretary
Katherine W. Davis
Katherine Llamas Finley
Deborah C. McPherson
Eva R. Ravenel

Reference Number:	367-16-DD
Title of Document:	Removable Media Security Policy
Date of Issue:	March 11, 2014
Effective Date:	March 11, 2014
Last Review Date:	March 11, 2014
Date of Last Revision:	March 11, 2014 **(NEW)**
Applicability:	All Divisions of Disabilities and Special Needs (DDSN) Employees

---

I. PURPOSE

The purpose of this policy is to establish security requirements and provide guidance to protect DDSN information, equipment and networks from security and privacy breaches that can occur with removable storage media such as flash drives, compact discs (CD), and other external storage devices.

II. SECURITY PROCEDURES AND REQUIREMENTS

1. The use of removable media, such as flash drives or CDs, to store DDSN data is, as a general rule, not permitted. Exceptions will only be made as noted below.

2. Exceptions to the no removable media rule will only be made at the request of executive management.

3. Upon receiving an approved exception request, the DDSN IT Division will issue an encrypted removable media device to be used only by the employee to which it is issued.

4. The physical security of a removable media device issued by the DDSN IT Division is the responsibility of the employee to which it is issued. The device must be kept in the employee's possession or stored in a secure location at all times.

5. Employees must not give or loan their assigned removable media device or encryption password to anyone else without IT Division approval and guidance.

6. Unencrypted DDSN data shall not be copied to or stored on removable media.

7. DDSN will utilize techniques which will not allow unencrypted data to be written to removable media from agency owned desktop and laptop computers.

8. All assigned removable media devices containing DDSN data must be returned to the IT Division for disposal. Disposing of a removable media device without returning it to the IT Division is not permitted.

9. If an assigned removable media device containing DDSN data becomes lost or stolen, the employee must notify the DDSN IT Division immediately through the helpdesk phone or email.

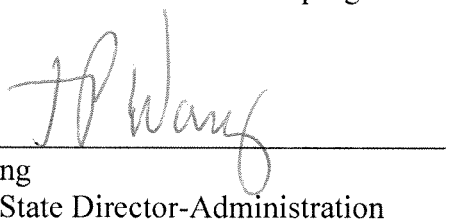
10. The employee must surrender any approved removable media device to the IT Division upon request and allow the device to be sanitized and all agency data removed.

III. IMPLEMENTATION, MAINTENANCE, AND COMPLIANCE

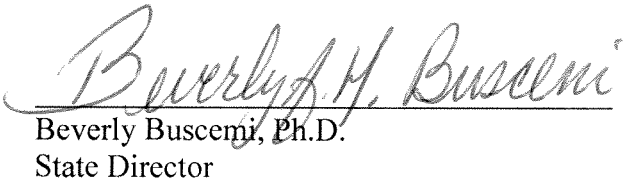
1. DDSN's designated Information Security Officer is responsible for insuring that this policy is implemented and communicated throughout the DDSN.

2. Any modifications to this policy shall be developed by the Information Security Officer and follow the normal course of approval for DDSN directives.

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



Tom Waring
Associate State Director-Administration
(Originator)



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