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

Reference Number:	367-21-DD	
Title of Document:	Data Protection and Privacy Policy	
Date of Issue:	October 5, 2015	
Effective Date:	October 5, 2015	
Last Review Date:	October 5, 2015	
Date of Last Revision:	July 13, 2016	**(NEW)**
Applicability:	All DDSN Employees	

DATA CLASSIFICATION

The purpose of the data classification section is to define the different categories for DDSN information assets regardless of form whether it is electronic, hard copy, or intellectual property.

Security Categorization (RA 2)

DDSN shall categorize data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. DDSN data shall be classified into one of the following categories:

1. Public

   Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.

2. Internal Use

Information that is used in daily operations of the DDSN. Examples of internal use information include DDSN hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the State.

3. Confidential

Confidential information refers to sensitive information in custody of the DDSN. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.

4. Restricted

Restricted information is highly sensitive information in custody or owned by the DDSN and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of restricted data shall result in considerable risk to the State including statutory penalties.

Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or DDSN Information Security and/or Data Privacy team(s) to determine the appropriate data classification.

If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.

Guidance *NIST SP 800-53 Revision 4: RA 2 Security Categorization*

DATA DISPOSAL

Policy Media Sanitization (MP 6)

DDSN shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse and release outside of the DDSN based on applicable regulatory requirements.

DDSN shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.

DDSN shall establish controls mechanism and processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.

DDSN shall implement controls to track media sanitization and disposal process, wherein such actions shall be tracked, documented, and verified.

Media sanitization documentation shall provide a record of the media sanitized, when, how media was sanitized, the individual who performed the sanitization, and the final disposition of the media. The record of action taken shall be maintained in a written or electronic format.

DDSN shall test media sanitization equipment and procedures at least annually to ensure correct performance.

DDSN shall define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be redeployed outside of the DDSN.

Approved processes like physical destruction or digital degaussing shall be performed on devices, before they are disposed.

DDSN shall destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.

The DDSN information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.

Guidance *NIST SP 800-53 Revision 4: MP 6 Media Sanitization*

DATA PROTECTION

Policy System and Communications Protection Policy and Procedures (SC 1)

The DDSN Information Security Officer and/or Data Privacy Officer shall be responsible for the development and implementation of policies and procedures to safeguard electronic protected, confidential, or restricted information.

DDSN employees shall follow DDSN's acceptable use policies when transmitting data.

Cryptographic Key Establishment and Management (SC 12)

DDSN shall implement mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users.

DDSN shall implement mechanisms to ensure the confidentiality of private keys.

DDSN shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization.

DDSN shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.

Cryptographic Protection (SC 17)

For Restricted or data protected by Federal or State laws or regulations: DDSN shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.

DDSN shall implement all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption.

DDSN shall not use any proprietary encryption algorithms for any purpose, unless approved by DDSN's information security department.

Transmission Confidentiality and Integrity (SC 8 and SC 9)

Confidential or restricted information transmitted as an email message shall be encrypted based on DDSN encryption policy.

Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with DDSN shall be encrypted or be transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN), point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).

DDSN shall implement wireless encryption standards such as Wi-Fi Protected Access 2 (WPA2), and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions that are used for transmitting confidential or restricted information.

DDSN shall utilize encrypted file transfer programs such as "secured File Transfer Protocol (SFTP)" (FTP over Secure Shell (SSH) and Secure Copy (SCP) to secure transfer of documents and data over the Internet. Only authorized users shall be able to initiate secure transactions.

Guidance: *NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures*
NIST SP 800-53 Revision 4: SC 8 Transmission Integrity
NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality
NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management
NIST SP 800-53 Revision 4: SC17 Cryptographic Protection

PRIVACY

Policy Privacy Impact Assessment

DDSN shall conduct a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII).

DDSN shall publish privacy policies on DDSN websites used by the public.

DDSN shall update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form).

PIAs shall include:

a. What information is to be collected (e.g., nature and source);
b. Why information is being collected (e.g., to determine eligibility)
c. Intended use of information (e.g., to verify existing data);
d. With whom the information will be shared;
e. What opportunities individuals have to decline to provide information;
f. How the information will be secured;

The PIA document shall be reviewed by a DDSN executive or designee, such as CIO, CISO, or similar.

DDSN shall provide a confidentiality agreement defining the responsibilities of the DDSN's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information.

The DDSN electronic information privacy officer, in conjunction with the DDSN human resources department, is responsible for the development and administration of this confidentiality agreement.

Guidance: *Fair Information Practice Principles (FIPPs)*
OMB Memorandum 03-22

Tom Waring
Associate State Director-Administration
(Originator)

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

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