Mary Poole
State Director
Patrick Maley
Deputy Director
Rufus Britt
Associate State Director
Operations
Susan Kreh Beck
Associate State Director
Policy
W. Chris Clark
Chief Financial Officer

SOUTH CAROLINA
Department
OF
Disabilities
AND
Special Needs

3440 Harden Street Extension
Columbia, South Carolina 29203
803/898-9600
Toll Free: 888/DSN-INFO
Home Page: www.ddsn.sc.gov

Reference Number:	367-32-DD	
Title of Document:	Information Security and Privacy	
Date of Issue:	November 19, 2020	
Effective Date:	November 19, 2020	
Last Review Date:	November 19, 2020	
Date of Last Revision:	November 19, 2020	**(NEW)**
Applicability:	DDSN Employees, DDSN Operated Community Settings, DSN Boards and Contracted Service Providers	

PURPOSE

The purpose of this directive is to set forth the South Carolina Department of Disabilities and Special Needs' (DDSN) Information Security and Privacy policy requirements consistent with South Carolina state law contained in recurring Provisos 117.113 (2014) and 101.32 (2014) and any successive statutes. State law requires all South Carolina state agencies, including institutions, departments, divisions, boards, commissions, and authorities, to implement the South Carolina Division of Information Security's Information Security and Privacy Standards, commonly identified as SCDIS-200.

BACKGROUND

Within statutory scope, these SCDIS-200 Standards apply to:

- All persons managed by an agency, such as employees, contractors, and volunteers.

- All agency information systems, regardless of location or service level agreement.

- All information contained on any agency information system, regardless of format or medium.

- All information otherwise under the control of any agency, regardless of format or medium.

The SCDIS-200 is comprised of 343 information and privacy control requirements for state agencies to implement. The South Carolina Division of Information Security organized these 343 requirements into 13 "control family" templates for state agency use to set out a logical framework for agencies to implement requirements.

POLICY

The DDSN has adopted and must implement the SCDIS-200 Standards in their entirety unless a business risk acceptance has been fully documented and approved by the State Director.

DDSN's Information Security Office will develop information security and privacy procedures to implement SCDIS-200 Standards to protect the availability, integrity, and confidentiality of DDSN Information Technology (IT) resources. While these directives apply to all staff, they are primarily applicable to Data Stewards; those managing the access to data and IT resources; and those using DDSN IT resources.

DDSN adopts the South Carolina Division of Information Security's 13 "control family" requirement templates (Appendices A-M) and added two additional requirement documents (Appendices N and O) to be used as the operating framework to meet minimum SCDIS-200 Standards. These requirement documents are contained in the following Appendices:

DDSN expects all employees and users to adhere to the requirements set forth in this directive as described fully in the attached appendices. No set of requirements can address all scenarios of IT security; therefore, these requirements address the most common aspects of information security.

IMPLEMENTATION, MAINTENANCE AND COMPLIANCE

1. DDSN's designated Chief Information Security Officer (CISO) is responsible for ensuring this directive is implemented and communicated throughout DDSN.

2. The CISO is responsible for ensuring that each control owner has developed operating procedures to implement all requirements. These operating procedures will be organized and made easily accessible to users, both internal to DDSN and the external provider network.

3. The CISO is responsible for ensuring compliance with SCDIS-200 requirements. The CISO will periodically, but no less than twice annually, provide a written report to executive management on the compliance status of all SCDIC-200 requirements, as well as provide a risk matrix (occurrence and consequence) of the control requirement families or other logical categorization of information security and privacy activity.

4. Any revisions to this directive shall be developed by the Information Security Office and follow the normal approval process according to DDSN Directive 100-01-DD: Electronic Communications Systems.

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

Barry D. Malphrus
Vice Chairman

Gary C. Lemel
Chairman

APPENDIX A

Information Security - Program

1. Information Security Program Planning

   a. Information Security Plan (PM 1)

      i. DDSN shall develop and communicate an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.

      ii. DDSN's security plan shall identify and assign security program roles, responsibilities, and management commitment, and ensure coordination among the agency's business units, as well as compliance with the security plan.

      iii. DDSN shall ensure coordination among the agency's business units responsible for the distinct aspects of information security (i.e., technical, physical, personnel, etc.).

      iv. DDSN shall ensure that the security plan is approved by senior management.

      v. DDSN shall review the information security plan at least on an annual basis.

      vi. DDSN shall update the security plan to address changes and problems identified during plan implementation or security control assessments.

      vii. DDSN shall protect the information security plan from unauthorized disclosure and modification

   b. Information Security Resources (PM 3)

      i. DDSN shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.

   c. Plan of Action and Milestones Process (PM 4)

      i. DDSN shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.

      ii. DDSN shall review plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

d. Information Security Measures of Performance (PM 6)

i. DDSN shall develop, monitor, and report on the results of information security measures of performance, as directed or guided by the South Carolina Division of Information Security (SCDIS) and the South Carolina Enterprise Privacy Office (SCEPO).

e. Guidance:

i. NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan
ii. NIST SP 800-53 Revision 4: PM 3 Information Security Resources
iii. NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process
iv. NIST SP 800-53 Revision 4: PM 6 Measures of Performance

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

2. Security Organization (Roles and Responsibilities)

a. Information Security Authority (2.2.3.1)

i. DDSN's chief executive shall ensure that the agency's senior officials are given the necessary authority to secure the operations and assets under their control.

b. Information Security Liaison (PM 2)

i. DDSN shall appoint an information security liaison with the mission and resources to coordinate, develop, implement, and maintain an information security plan.

c. Information Security Workforce (PM 13)

i. DDSN shall establish an information security workforce and professional development program appropriately sized to the agency's information security needs.

d. Role-based Security Training (AT 3)

i. DDSN shall provide role-based security training to personnel with assigned security roles and responsibilities.

e. Guidance:

i. NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer
ii. NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
iii. NIST SP 800-53 Revision 4: AT 3 Role-based Security Training
iv. NIST SP 800-100: 2.2.3.1 Agency Head

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

3. Policy Management (Plan of Action)

   a. Procedure Development

      i. DDSN shall adopt a risk-based approach to identify State, Federal and agency-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.

      ii. DDSN shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.

      iii. DDSN shall approach independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.

      iv. DDSN shall work in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.

      v. Information security procedures that are developed at the agency shall contain the following information, as appropriate:

         1. Revision history
         2. Introduction
         3. Preface
         4. Ownership, roles, and responsibilities
         5. Purpose
         6. Policy statements
         7. Policy supplement
         8. Guidance
         9. Definitions

      vi. Scenarios which cannot be effectively addressed within the constraints of the agency's security procedures, should be identified as exceptions:

         1. Exceptions shall be evaluated in the context of potential risk to the agency as a whole;
         2. Exceptions that create significant risks without adequate compensating controls shall not be approved; and
         3. Exceptions shall be consistently evaluated in accordance with the agency's risk acceptance practice.

vii. DDSN shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.

viii. DDSN shall identify gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

ix. DDSN shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.

x. DDSN shall review procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State's risk posture.

b. Procedure Review and Approval

i. A procedure governance committee shall be established for the purpose of review and approval of procedures.

ii. Procedure exemptions shall be explicitly approved by the procedure governing committee.

iii. Procedure approval history shall be documented in detail.

c. Procedure Implementation

i. DDSN shall implement mechanisms to help ensure that information security procedures will be available to the agency's personnel on a continuous basis and whenever required.

ii. DDSN shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

d. Guidance:

i. NIST SP 800-53 Revision 4: PM 6 Measures of Performance

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

4. Information Security Controls Deployment

a. Controls Deployment

i. DDSN shall adopt a risk-based approach to prioritize deployment of controls.

ii. DDSN shall allocate the appropriate subject matter experts to the deployment of State, Federal and agency-specific information security controls.

iii. DDSN shall approach independent external (third party) specialists to assist in the deployment of information security controls in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.

iv. Controls which cannot be deployed due to the agency's resource or other constraints must be reported to the office of the State Chief Information Security Officer.

v. DDSN shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.

vi. DDSN shall identify gaps within the controls that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.

vii. DDSN shall develop and implement a communication plan to disseminate new controls or changes to existing controls.

viii. DDSN shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

APPENDIX B

Information Security - Access Control

1. Access Management

a. The purpose of the access management section is to establish processes to control access and use of DDSN information resources. Access management incorporates role-based access controls (RBAC), privileged user access, access definitions, roles, and profiles.

b. Access Control Policy and Procedures (AC 1)

i. DDSN shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

c. Account Management (AC 2)

i. DDSN shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.

ii. DDSN shall identify authorized users of information systems and specify access rights.

iii. Requests for access to DDSN Data must be approved by the business/data owner (or delegate) prior to provisioning the user account.

iv. DDSN shall authorize and monitor the use of guest/anonymous and temporary accounts, and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required.

v. DDSN shall utilize request for access change documentation (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.

vi. DDSN shall remove or disable default user accounts and, if user accounts cannot be removed or disabled, they should be renamed.

vii. Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default.

viii. Access requests from users shall be recorded and follow the DDSN established approval process.

ix. DDSN shall ensure that user access requests are approved by a business owner (or any other pre-approved role).

x. Privileged accounts (e.g., system/network administrators having root level access, database administrators), shall only be allowed after approval by a DDSN information security officer and/or similarly designated role. The approval shall be granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason based on role requirements.

xi. DDSN shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.

xii. DDSN shall enforce periodic user access reviews to be performed by information/data owners or their assigned delegate(s) to ensure the following:

1. Access levels remain appropriate, based upon approvals;
2. Terminated employees do not have active accounts;
3. There are no group accounts, unless approved; and
4. There are no duplicate user identifiers.

xiii. DDSN shall review information system accounts within every 180 days and require annual certification.

xiv. DDSN shall regulate information system access and define security requirements for contractors, vendors, and other service providers.

xv. DDSN shall administer privileged user accounts in accordance with a role-based access model.

d. Access Enforcement (AC 3)

i. DDSN shall enforce approved authorizations for logical access to information systems.

ii. DDSN shall implement encryption as an access control mechanism if required by Federal, State, or other laws or regulations.

e. Information Flow Enforcement (AC 4)

i. For Restricted data: DDSN systems shall enforce data flow controls using security attributes on information, source, and destination objects as a basis for flow control decisions.

f. Separation of Duties (AC 5)

i. DDSN shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to:

1. Audit functions are not performed by security personnel responsible for administering information system access;
2. Divide critical business and information system management responsibilities;
3. Divide information system testing and production functions between different individuals or groups; and
4. Independent entity to conduct information security testing of information systems.

ii. DDSN shall document and implement separation of duties through assigned information system access authorizations.

g. Least Privilege (AC 6)

i. DDSN shall ensure that only authorized individuals have access to DDSN data/information and that such access is strictly controlled, audited in accordance with the concepts of "need-to-know, least-privilege, and separation of duties."

ii. DDSN shall implement processes or mechanisms to:

1. Disable file system access not explicitly required for system, application, and administrator responsibilities;
2. Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;
3. Restrict use of database management to authorized database administrators;
4. Grant access to authorized users based on their required job duties; and
5. Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.

h. Unsuccessful Login Attempts (AC 7)

i. DDSN systems shall enforce a limit of unsuccessful logon attempts during a DDSN-defined period. The number of logon attempts shall be commensurate with the classification of data hosted, processed, or transferred by the information system.

ii. DDSN shall automatically lock user accounts the after maximum logon attempts is reached. DDSN shall establish an account lock time period commensurate with the classification of data hosted, processed, or transferred by the information system.

i. System Use Notification (AC 8)

i. DDSN systems shall display the following warning before granting system access. "This system is solely for the use of authorized DDSN personnel. The information contained herein is the property of DDSN and subject to non-disclosure, security, and confidentiality requirements. DDSN shall monitor system usage for unauthorized activities. Any user accessing this system expressly consents to such monitoring."

j. Session Lock (AC 11)

i. DDSN systems shall time out sessions or require a re-authentication process after 30 minutes or less of inactivity.

k. Guidance:

i. NIST SP 800-53 Revision 4: AC 1 Access Control Policy and Procedures
ii. NIST SP 800-53 Revision 4: AC 3 Access Enforcement
iii. NIST SP 800-53 Revision 4: AC 4 Information Flow Enforcement
iv. NIST SP 800-53 Revision 4: AC 5 Separation of Duties
v. NIST SP 800-53 Revision 4: AC-6 Least Privilege
vi. NIST SP 800-53 Revision 4: AC 7 Unsuccessful Login Attempts
vii. NIST SP 800-53 Revision 4: AC 8 System Use Notification
viii. NIST SP 800-53 Revision 4: AC 11 Session Lock

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

2. Network Access Management

a. Remote Access (AC 17)

i. DDSN shall document allowed methods for remote access to the network and information systems.

ii. DDSN shall utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.

iii. Virtual Private Network (VPN) or equivalent encryption technology shall be used to establish remote connections with DDSN networks and information systems.

iv. Remote users shall connect to DDSN information systems only using mechanism protocols approved by the DDSN through a limited number of managed access control points for remote connections.

v. For Restricted data and/or system administrators: DDSN employees and authorized third parties accessing DDSN information systems remotely shall do so via an approved two-factor authentication (2FA) technology.

vi. DDSN shall develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required).

b. Wireless Access (AC 18)

i. DDSN establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.

ii. DDSN shall only use wireless networking technology that enforces user authentication.

iii. DDSN shall authorize wireless access to information systems prior to allowing use of wireless networks.

iv. DDSN does not allow wireless access points to be installed independently by users.

c. Use of External Information Systems (AC 20)

i. If external systems are authorized by the DDSN, the DDSN shall establish terms and conditions for their use, including types of applications that can be accessed from external information systems, security category of information that can be processed, stored, and transmitted, use of VPN and firewall technologies, the use and protection against the vulnerabilities of wireless technologies, physical security maintenance and the security capabilities of installed software are to be updated.

d. Boundary Protection (SC 7)

i. DDSN networks where information deemed critical by DDSN is stored or processed shall be physically or logically segregated from publicly available networks.

ii. DDSN networks and information systems shall not be accessible from public networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices.

iii. DDSN limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.

e. Guidance:

i. NIST SP 800-53 Revision 4: AC 17 Remote Access
ii. NIST SP 800-53 Revision 4: AC 18 Wireless Access
iii. NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
iv. NIST SP 800-53 Revision 4: SC 7 Boundary Protection

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

3. Identity Management

a. Identification and Authentication (IA 2, IA 4, AND IA 8)

i. DDSN shall establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators.

ii. DDSN shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.

iii. DDSN shall allow the use of group IDs only where these are necessary for business or operational reasons; group IDs shall be formally approved and documented.

iv. If DDSN requires group IDs, it shall require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID).

v. DDSN shall minimize the use of system, application, or service accounts; and DDSN shall document, formally approve, and designate a responsible party of this type of accounts.

vi. DDSN security system shall be able to identify and verify the identification and, if deemed necessary by DDSN, the location of each authorized user.

b. Guidance:

i. NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)
ii. NIST SP 800-53 Revision 4: IA 4 Identifier Management

iii. NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)

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

4. Authentication

a. Authenticator Management (IA 5)

i. DDSN shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user.

b. Unsuccessful Logon Attempts (AC 7)

i. DDSN shall implement mechanisms to record successful and failed authentication attempts.

c. Session Lock (AC 11)

i. DDSN shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems.

ii. DDSN networks and information systems shall disable user access upon reaching the maximum number of invalid access attempts as defined by the DDSN.

iii. Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.

d. Guidance:

i. NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts
ii. NIST SP 800-53 Revision 4: AC 11 Session Lock
iii. NIST SP 800-53 Revision 4: IA 5 Authenticator Management

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

5. Emergency Access

a. Policy Account Management (AC 2)

i. DDSN shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.

ii. The emergency procedures shall ensure that:

1. Only identified and authorized personnel are allowed access to live systems and data;
2. All emergency actions are documented in detail; and
3. Emergency action is reported to management and reviewed in an orderly manner.

iii. DDSN will establish a process to automatically terminate emergency accounts within 24 hours and temporary accounts with a fixed duration not to exceed 365 days.

b. Guidance:

i. NIST SP 800-53 Revision 4: AC 2 Account Management

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

6. Password Policy

a. Account Management (AC 2)

i. DDSN shall establish a process for password-based authentication to include the following:

1. Automatically force users (including administrators) to change user account passwords every 90 days.
2. Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every 60 days.
3. Passwords for system accounts to be changed at least every 180 days.
4. Enforce password minimum lifetime of one (1) day.
5. Prohibit the use of dictionary names or words as passwords.
6. Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters.
7. Enforce a minimum number of characters to be changed when new passwords are created. For Restricted data consider a minimum of four (4) changed characters.
8. Encrypt passwords in storage and during transmission.
9. Prohibit password reuse for six (6) generations prior to reuse.

ii. DDSN users shall not share passwords with others under any circumstance.

iii. System passwords shall be changed immediately upon termination/resignation of any employee with privileged access.

iv. DDSN shall not allow users to use common words or based on personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).

v. DDSN shall suspend user accounts after a specified number of days of inactivity.

vi. DDSN shall implement a process to change passwords immediately if there is reason to believe a password has been compromised or disclosed to someone other than the authorized user.

b. Guidance:

i. NIST SP 800-53 Revision 4: AC 2 Account Management

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

7. Password Administration

a. Policy Access Agreements (PS 6)

i. DDSN users shall sign an acknowledgement to evidence understanding of authentication policies, including the DDSN policy to keep passwords confidential and to keep group passwords solely within the members of the group.

ii. DDSN shall require that employees sign acknowledgement prior to allowing access to network and information systems.

b. Identification and Authentication (IA 2, IA 6, and IA 8)

i. DDSN shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password.

ii. DDSN shall establish a process to uniquely identify and authenticates non-Agency users.

iii. DDSN shall establish procedures to manage new or removed privileged accounts passwords.

c. Authenticator Management (IA 5)

i. First-time passwords shall be set to a unique value per user and changed immediately after first use.

ii. DDSN shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.

iii. DDSN shall not allow default passwords for network and remote applications.

d. Authenticator Feedback (IA 6)

i. DDSN shall obscure feedback of authentication information during the authentication process to protect the information from exploitation/use by unauthorized individuals.

e. Guidance:

i. NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)
ii. NIST SP 800-53 Revision 4: IA 5 Authenticator Management
iii. NIST SP 800-53 Revision 4: IA 6 Authenticator Feedback
iv. NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)
v. 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

APPENDIX C

Information Security - Asset Management

1. Access Identification

a. Information System Component Inventory (CM 8)

i. DDSN shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a system/business owner, a data classification, and a description of the location of the asset. Examples of assets associated with information systems are:

1. Information assets: databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information.
2. Software assets: application software, system software, development tools and utilities.
3. Physical assets: physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks).
4. Services: computing and communications services.

ii. Access to DDSN assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.

iii. DDSN shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.

b. Security Impact Analysis (CM 4)

i. DDSN shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.

ii. DDSN shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.

c. Guidance:

i. NIST SP 800-53 Revision 4: CM 4 Security Impact Analysis
ii. NIST SP 800-53 Revision 4: CM 8 Information System Component Inventory

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

APPENDIX D

Information Security - Business Continuity Management

1. Contingency Planning

   a. Contingency Planning Policy and Procedures (CP 1)

      i. DDSN shall establish a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

      ii. DDSN shall establish formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.

      iii. DDSN shall establish a formal process for annual contingency planning policy and procedure review and update.

   b. Contingency Plan (CP 2, CP 7)

      i. DDSN shall conduct a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the DDSN and determine a point in time (i.e., recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the DDSN.

      ii. DDSN shall utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications.

      iii. DDSN shall assign contingency roles and responsibilities to key individuals from all business functions.

      iv. DDSN shall establish procedures to maintain continuity of critical business functions despite critical information system disruption, breach, or failure.

      v. DDSN shall document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable the DDSN to respond to potential disruptions and recover its critical business functions within a predetermined RTO following a disruption.

      vi. DDSN shall establish a process to ensure that the BCP is reviewed and approved by senior management.

vii. DDSN shall distribute copies of the BCP to key personnel responsible for the recovery of the critical business functions and other relevant personnel and partners with contingency roles, as determined by the DDSN.

viii. DDSN shall establish and implement procedures to review the BCP at planned intervals and at least on an annual basis.

ix. DDSN shall establish a process to update the contingency plan, including BIA, when changes to the organization, information system, or environment of operation occurred.

c. Contingency Training (CP 3)

i. DDSN shall provide training to personnel with assigned contingency roles and responsibilities.

ii. DDSN shall establish a process for identifying and delivering training requirements (i.e., frequency) to and from the relevant participants and evaluating the effectiveness of its delivery.

iii. DDSN shall incorporate simulated events and lessons learned into contingency training to facilitate effective response by personnel with contingency roles when responding to disruption.

d. Contingency Plan Testing (CP 4)

i. DDSN shall test the BCP at least annually to determine the effectiveness of the plan and the DDSN readiness to execute the plan.

ii. DDSN shall review the BCP test results, record lessons learned and perform corrective actions as needed.

iii. DDSN shall employ standard testing methods, ranging from walk-through and tabletop exercises to more elaborate parallel/full interrupt simulations, to determine the effectiveness of the plan and to identify potential weaknesses in the plans.

e. Criticality Analysis (SA 14)

i. DDSN shall establish procedures to enable continuation of critical business operations while operating in emergency mode.

f. Guidance:

i. NIST SP 800-53 Revision 4: CP 1 Contingency Planning Policy and Procedures

ii. NIST SP 800-53 Revision 4: CP 2 Contingency Plan
iii. NIST SP 800-53 Revision 4: CP 3 Contingency Training
iv. NIST SP 800-53 Revision 4: CP 4 Contingency Plan Testing
v. NIST SP 800-53 Revision 4: SA 14 Criticality Analysis

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

2. Disaster Recovery and Contingency Strategies

a. Disaster Recovery Plan (CP 2)

i. DDSN shall develop a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.

ii. DDSN shall establish recovery time objectives for the BIA identified critical information systems.

iii. DDSN shall establish and document procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.

iv. DDSN shall assign disaster recovery roles and responsibilities to key individuals.

v. DDSN shall establish a process to ensure that the DRP is reviewed and approved by senior management.

vi. DDSN shall distribute copies of the DRP to key personnel responsible for the recovery of the critical information systems and other relevant personnel and partners with contingency roles, as determined by the DDSN.

vii. DDSN shall establish and implement procedures to review the DRP at planned intervals and at least on an annual basis.

viii. DDSN shall establish a process to update the DRP when changes to the organization or environment of operation occurred.

b. Alternate Site (CP 7)

i. DDSN shall identify and establish processes to relocate to an alternate site to facilitate the resumption of information system operations for business-critical functions within the defined recovery objectives (RTO and

Recovery Point Objective (RPO)) when the primary site is unavailable due to disruption.

ii. DDSN shall ensure that equipment and supplies required to resume operations at the alternate processing site are available.

iii. DDSN shall ensure contracts are in place with third parties and suppliers to support delivery to the site within the defined time period for transfer/ resumption of critical business operations.

iv. DDSN shall ensure that the alternate processing site provides information security safeguards similar to that of the primary site.

v. DDSN shall identify potential accessibility problems to the alternate site in the event of an area-wide disruption or disaster.

c. Telecommunications Services (CP 8)

i. DDSN shall establish primary and alternate telecommunication service agreements with priority-of-service provisions in accordance with organizational availability requirements (including RTOs), quality of service and access.

ii. DDSN shall establish alternate telecommunications services to facilitate the resumption of information system operations for critical business functions within the defined recovery objectives when the primary telecommunications capabilities are unavailable.

iii. DDSN shall require primary and alternate telecommunication service providers to have contingency plans.

iv. Information System Recovery and Reconstitution (CP 10).

v. DDSN shall establish documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.

vi. DDSN shall implement procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.

vii. DDSN shall provide the capability to restore information system components within defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components (for e.g. reimaging methods).

viii. DDSN shall establish measures to protect backup and restoration hardware, firmware, and software.

d. Guidance:

i. NIST SP 800-53 Revision 4: CP 7 Alternate Processing Site
ii. NIST SP 800-53 Revision 4: CP 8 Telecommunications Services
iii. NIST SP 800-53 Revision 4: CP 10 Information System Recovery and Reconstitution

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

3. Data Backups

a. Data Backup and Storage Policy

i. DDSN shall develop, maintain, and document a Data Backup and Storage Policy that address the adequate procedures to storage data and thus ensure the recovery of electronic information in the event of failure.

ii. DDSN shall identify and apply security requirements for protecting data backups based on the distinct types of data (sensitive, confidential, public) handle by the entity.

b. Alternate Storage Site (CP 6)

i. DDSN shall identify an alternate storage site that is separated from the primary site so as not to be susceptible to same hazards to storage and recover information system backup information.

ii. DDSN shall establish necessary agreements with the site/location owner to ensure that data storage and retrieval process are not hindered during or post an incident.

iii. DDSN shall ensure that the alternate storage site provides information security safeguards similar to that of the primary storage site.

iv. DDSN shall identify potential accessibility problems to the alternate storage site in the event of a disruption or disaster.

v. DDSN shall identify secure transfer methods when transporting backup media off-site.

vi. DDSN shall establish and maintain an authorization list to retrieve backups from the off-site location.

vii. DDSN shall review on an annual basis the security of the off-site location to ensure data is unexposed to unauthorized disclosure or modification while in storage.

c. Information System Backup (CP 9)

i. DDSN shall establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.

ii. DDSN shall establish a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.

iii. DDSN shall establish safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.

iv. DDSN shall identify encryption/secure methods in storage of backup data to transportable media (i.e., tapes, CD Rooms, etc.).

v. DDSN shall enforce dual authorization ("two-person control") for the deletion or destruction of DDSN sensitive data.

d. Guidance:

i. NIST SP 800-53 Revision 4: CP 6 Alternate Storage Site
ii. NIST SP 800-53 Revision 4: CP 9 Information System Backup

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

APPENDIX E

Human Resource and Security Awareness

1. Human Resource Compliance

    a. Personnel Security Policy and Procedures (PE 1)

        i. DDSN shall define security roles and responsibilities of employees, contractors and third-party users and shall be documented in accordance with DDSN information security policies.

    b. Personnel Screening and Third-Party Personnel Security (PS 3) and (PS 7)

        i. DDSN shall conduct background verification checks on all candidates for employment, including contractors, and third party users, which shall be carried out in accordance with relevant laws and DDSN Directive 406-04-DD: Criminal Record Checks and Reference Checks of Direct Caregivers.

    c. Personnel Termination and Transfer (PS 4) and (PS 5)

        i. Upon termination/transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel shall return to DDSN all agency documents (and all copies thereof) and other agency property and materials in their possession or control.

    d. Access Agreements (PS 6)

        i. As part of their information security obligation, employees, contractors and third party users shall agree and sign the Acceptable Use of Network Services and the Internet Form (DDSN Directive 367-09-DD), which shall state responsibilities for information security.

    e. Guidance:

        i. NIST SP 800-53 Revision 4: PE 1 Personnel Security Policy and Procedures
        ii. NIST SP 800-53 Revision 4: PS 3 Personnel Screening
        iii. NIST SP 800-53 Revision 4: PS 4 Personnel Termination
        iv. NIST SP 800-53 Revision 4: PS 5 Personnel Transfer
        v. NIST SP 800-53 Revision 4: PS 6 Access Agreements
        vi. NIST SP 800-53 Revision 4: PS 7 Third-Party Personnel Security

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

2. Security Awareness Training

a. Security Awareness Training and Information Security Workforce (AT 2) and (PM 13)

i. DDSN management shall require employees, contractors, and third-party users to apply security in accordance with established policies and procedures of the organization.

b. Role-Based Security Training (AT 3)

i. DDSN shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to contractors and third-party users, as relevant for their job function.

ii. Training must be accompanied by an assessment procedure based on the cyber security training content presented to determine comprehension of key cyber security concepts and procedures.

iii. User access to DDSN information assets and systems will only be authorized for those users whose cyber security awareness training is current (e.g., having passed the most recent required training stage).

c. Testing, Training, and Monitoring (PM 14)

i. DDSN will appoint a cyber-security awareness training coordinator to manage training content, schedules, and user training completion status.

ii. The DDSN cyber security training coordinator, along with the Information Security Officer will review training content on an annual basis to ensure that it aligns with State of South Carolina policies.

d. Guidance:

i. NIST SP 800-53 Revision 4: AT 2 Security Awareness Training
ii. NIST SP 800-53 Revision 4: AT 3 Role-Based Security Training
iii. NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
iv. NIST SP 800-53 Revision 4: PM 14 Testing, Training, and Monitoring

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

APPENDIX F

Information Security Information Systems Acquisitions, Development, and Maintenance

1. Change Management

a. Configuration Change Control (CM 3)

i. DDSN shall define change management controls to manage changes to information systems to minimize the likelihood of disruption, unauthorized alterations, and errors. The implementation of changes shall be controlled using a change control process. The following recommendations shall be followed for the change control process:

1. All requests for change shall be managed in a structured way that determines the impact on the operational system and its functionality;
2. All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner;
3. DDSN shall have a process to categorize, prioritize and authorize changes to information systems;
4. Post-implementation reviews shall be performed to ensure production changes are operating as intended;
5. A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;
6. A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; and
7. Information systems shall be reviewed and tested after major changes to operating systems.

b. Guidance:

i. NIST SP 800-53 Revision 4: CM 3 Configuration Change Control

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

2. Configuration Management

a. Policy Baseline Configuration (CM 2)

i. DDSN shall develop, review, and formally approve baseline configurations (most secure state) for critical information systems and infrastructure components.

ii. DDSN shall develop a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.

iii. DDSN shall establish a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.

iv. DDSN shall retain older versions of baseline configurations to be able to support rollback.

v. DDSN shall review and update baseline configurations periodically, and/or as an integral part of information system component installations or upgrades.

b. Configuration Management Plan (CM 9)

i. The DDSN shall assign responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.

c. Guidance

i. NIST SP 800-53 Revision 4: CM 2 Baseline Configuration
ii. NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan
iii. NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems

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

3. System Development and Maintenance

a. Policy System Security Plan (PL 2)

i. DDSN shall prepare system security plans and documentation for critical enterprise information systems or systems under development.

ii. System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.

iii. When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

b. Vulnerability Scanning (RA 5)

i. DDSN shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes before the systems are moved into production.

ii. DDSN shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.

iii. Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.

c. System and Services Acquisition Policy and Procedures (SA 2)

i. DDSN shall develop and follow a set of procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.

ii. DDSN shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

d. System Development Life Cycle (SA 3)

i. DDSN shall implement appropriate security controls at all stages of the information system life cycle.

e. External Information System Services (SA 9)

i. DDSN shall supervise and monitor outsourced software development to validate DDSN security requirements.

f. Developer Security Testing and Evaluation (SA-11)

i. DDSN shall establish separate development, testing, and production environments.

ii. DDSN shall not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval, procedures to remove/delete data after completion of tests, and documentation of activities, shall be implemented.

g. Flaw Remediation (SI 2)

i. DDSN shall design appropriate controls into information systems, including user developed applications to ensure correct processing.

ii. DDSN shall ensure that software patches are applied when they function to remove or reduce security weaknesses.

h. Security Alerts, Advisories, and Directives (SI 5)

i. DDSN shall establish a process to collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.

ii. A specific group or individual shall be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

i. Software, Firmware, and Information Integrity (SI 7)

i. DDSN shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

ii. DDSN shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

j. Information Input Validation (SI 10)

i. DDSN shall incorporate controls into information systems to check the validity of information inputs and information outputs.

ii. DDSN shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

k. Session Authenticity (SC 23)

i. DDSN shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

l. Policy Supplement

i. Threat and Vulnerability Management 1.1: Patch Management

ii. Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution

m. Guidance:

i. NIST SP 800-53 Revision 4: PL 2 System Security Plan
ii. NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
iii. NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure
iv. NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle
v. NIST SP 800-53 Revision 4: SA 9 External Information System Services
vi. NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation
vii. NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
viii. NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity
ix. NIST SP 800-53 Revision 4: SI 10 Information Input Validation
x. NIST SP 800-53 Revision 4: SC 23 Session Authenticity

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

4. Release Management

a. Policy Allocation of Resources (SA 2)

i. DDSN shall ensure that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build, and test, pilot, and deploy).

ii. DDSN shall determine as part of the release planning process:

1. Resources required to deploy the release;
2. Pass/fail criteria;
3. Build and test plans prior to implementation;
4. Pilot and deployment plans; and
5. Develop requirements for the release.

b. Information System Documentation (SA 5)

i. DDSN shall document the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release.

ii. DDSN shall validate the release design against the requirements and identify the risks and potential issues.

c. Security Engineering Principles (SA 8)

i. DDSN shall implement standardization and enforce operational controls using change requests for deploying releases into production.

d. Guidance:

i. NIST SP 800-53 Revision 4: SA 2 Allocation of Resources
ii. NIST SP 800-53 Revision 4: SA 5 Information System Documentation
iii. NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles

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

APPENDIX G

Information Security - IT Compliance

1. Audit and Compliance

a. Compliance with Legal and Contractual Requirements (A.15.1)

i. DDSN shall identify and document its obligations to applicable State, federal and other third-party laws, and regulations in relation to information security.

b. Compliance with Security Policies and Standards (A.15.2.1, A.15.2.2)

i. At least annually, DDSN shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.

ii. Results from compliance reviews or audits shall be documented and reported to DDSN leadership.

c. Audit and Accountability Policy and Procedures (AU 1)

i. DDSN shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures.

ii. DDSN shall implement a process to review and update the audit and accountability policy and associated procedures at least annually.

d. Guidance:

i. ISO 27001:2005: A.15.1 Compliance with legal and contractual requirements
ii. ISO 27001:2005: A.15.2.1 Compliance with security policies and standards
iii. ISO 27001:2005: A.15.2.2 Technical compliance checking
iv. NIST SP 800-53 Revision 4

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

2. Information System Audit Considerations

a. Information Systems Audit Controls (A.15.3.1)

i. DDSN shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

b. Protection of information systems audit tools (A.15.3.2)

i. DDSN shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.

c. Audit Events (AU 2)

i. DDSN shall determine the type of events that are to be audited within information systems.

ii. DDSN shall review and update the list of audited events annually.

iii. DDSN leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.

d. Content of Audit Records (AU 3)

i. DDSN information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

e. Audit Records Review and Reporting (AU 6)

i. DDSN shall analyze information system audit records periodically.

ii. DDSN shall report findings of audit records reviews to information security personnel and DDSN leadership.

iii. DDSN shall perform correlation and analysis of information generated by security assessments and monitoring.

f. Audit Storage Capacity (AU 4)

i. DDSN shall allocate sufficient audit storage capacity to help ensure compliance with audit logs retention requirements from State, federal, and other applicable third-party laws, and regulations.

ii. DDSN shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.

g. Guidance:

i. ISO 27001:2005: A.15.3.1 Information systems audit controls

ii. ISO 27001:2005: A.15.3.2 Protection of information systems audit tools
iii. NIST SP 800-53 Revision 4: AU 2 Audit Events
iv. NIST SP 800-53 Revision 4: AU 3 Content of Audit Records
v. NIST SP 800-53 Revision 4: AU 4 Audit Storage Capacity
vi. NIST SP 800-53 Revision 4: AU 6 Audit Review, Analysis, and Reporting

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

APPENDIX H

Information Security - IT Risk Strategy

I. Security Performance and Metrics

a. Information Security Measures of Performance (PM 6)

i. DDSN shall develop, monitor, and report on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.

ii. DDSN-defined performance measures should be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement.

b. Manageability of Metrics (3.4.2)

i. DDSN shall ensure that the metrics/ measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps.

c. Data Management Concerns (3.4.3)

i. DDSN shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

d. Guidance:

i. NIST SP 800-53 Revision 4: PM 6 Information Security Measures of Performance
ii. NIST SP 800-55 Revision 1: 3.4.2 Manageability
iii. NIST SP 800-55 Revision 1: 3.4.3 Data Management Concerns

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

2. Third Party Risk Management

a. External Information System Services (SA 9)

i. DDSN shall establish a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

ii. DDSN shall implement processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis.

b. Risk Assessment (RA 3)

i. DDSN shall establish a process to conduct risk assessments on third party service providers and document the risk assessment results.

ii. DDSN shall implement controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties.

c. System Interconnections (CA 3)

i. DDSN shall authorize connections from DDSN information systems to third party information systems by entering into Interconnection Security Agreements.

ii. For each third-party interface, DDSN shall document the interface characteristics, security requirements, and the nature of the information communicated.

d. Use of External Information Systems (AC 20)

i. DDSN shall establish terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.

ii. Terms and conditions established by DDSN should control:

1. Access to DDSN information systems from third party information systems; and
2. Controls for processing, storing, or transmit of DDSN data using third party information systems.

iii. DDSN shall review and update third party security agreements on an annual basis, or as defined in the contract.

e. Information Sharing with Third Parties (UL 2)

i. DDSN shall share personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.

ii. DDSN shall, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used.

iii. DDSN shall monitor, audit, and train its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data.

iv. DDSN shall evaluate any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

f. Guidance:

i. NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
ii. NIST SP 800-53 Revision 4: CA 3 System Interconnections
iii. NIST SP 800-53 Revision 4: PS 6 Access Agreements
iv. NIST SP 800-53 Revision 4: RA 3 Risk Assessment
v. NIST SP 800-53 Revision 4: SA 9 External Information System Services
vi. NIST SP 800-53 Revision 4: UL 2 Information Sharing with Third Parties

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

APPENDIX I

Mobile Device Security

1. Security Procedures and Requirements

   a. 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).

   b. 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.

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

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

   e. 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.

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

   g. 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.

   h. 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.

   i. 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.

j. 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.

k. 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.

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

m. 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).

2. Mobile Device Access Agreement

a. 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.

b. 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.

c. 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.

Mobile Device Access Agreement

South Carolina Department of Disabilities and Special Needs

1. EMPLOYEE

By signing below, I am requesting to use my personal mobile device to access DDSN data including, but not limited to, agency email. I agree to abide by the procedures and requirements of the DDSN Mobile Device Security Policy & DDSN Access Control Policy.

I understand that the policy includes, but is not limited to, the following:

➢ I agree that the physical security of the device is my responsibility and I will keep it in my physical possession whenever possible and store it in a secure place when it is not in my possession.

➢ I agree to notify the DDSN 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.

➢ I agree to notify the DDSN IT Division immediately if my device becomes lost or stolen.

➢ I grant DDSN the right to install the DDSN mobile device management agent on my device.

➢ I grant DDSN the right to remotely wipe or erase data from my device should it be deemed necessary in order to protect the security and privacy of DDSN data. This may include loss of personal data stored on the device.

➢ I am aware that the use of this software is at my own risk, DDSN is not responsible for non-functioning or bricked devices, non-working SD cards, batteries or warranty void.

______________________________ ______________________________
Print Employee Name Signature

2. MANAGER

I certify that the above signed employee has a valid business need to access DDSN data using a mobile device.

______________________________ ______________________________
Print Manager Name Signature

Date: ______________________________

Please return this form to: Kareem Briggs, Chief Information Security Officer by email at *kareem.briggs@ddsn.sc.gov or by fax to (803) 898-9658*

APPENDIX J

Physical Access and Environmental Security

1. Physical Security

a. Physical and Environmental Protection Policy and Procedures

i. DDSN shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.

ii. DDSN shall establish procedures to review and maintain current the physical and environmental protection policy and associated procedures.

b. Physical Access Authorizations

i. DDSN shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.

ii. DDSN shall establish a process to review, approve, and issue credentials for facility access.

iii. DDSN shall remove individuals from the facility access list when access is no longer required.

c. Physical Access Control

i. DDSN control entry to/exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).

ii. DDSN shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.

iii. DDSN shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.

iv. DDSN shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.

v. DDSN shall establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.

vi. DDSN shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

d. Access Control for Transmission Medium

i. DDSN shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).

e. Access Control for Output Devices

i. DDSN shall place output devices in secured areas and in locations that can be monitored by authorized personnel and allow access to authorized individuals only.

ii. DDSN shall control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.

f. Monitoring Physical Access

i. DDSN shall review physical access logs at a defined frequency and upon occurrence of security incidents.

g. Visitor Access Records

i. DDSN shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of one (1) year.

h. Delivery and Removal

i. DDSN shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

2. Environmental Security

a. Policy Power Equipment and Cabling

i. DDSN shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.

b. Emergency Shutoff

i. DDSN shall make available the capability of shutting off power to data center(s) during an incident.

ii. DDSN shall place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.

iii. DDSN shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.

c. Data Center Emergency Power

i. DDSN shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.

d. Data Center Fire Protection

i. DDSN shall install and maintain fire detection and suppression devices that are supported by an independent power source.

ii. DDSN shall employ fire detection devices/system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.

iii. DDSN shall employ an automatic fire suppression system if/when the data center(s) is not staffed on a continuous basis.

e. Data Center Temperature and Humidity Controls

i. DDSN shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.

ii. DDSN shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.

f. Data Center Water Damage Protection

i. DDSN shall protect processing equipment from damage resulting from water leakage.

g. Guidance:

i. NIST SP 800-53 Revision 4: PE 1 Physical and Environmental Protection Policy and Procedures
ii. NIST SP 800-53 Revision 4: PE 2 Physical Access Authorizations
iii. NIST SP 800-53 Revision 4: PE 3 Physical Access Control

iv. NIST SP 800-53 Revision 4: PE 4 Access Control for Transmission Medium

v. NIST SP 800-53 Revision 4: PE 5 Access Control for Output Devices

vi. NIST SP 800-53 Revision 4: PE 6 Monitoring Physical Access

vii. NIST SP 800-53 Revision 4: PE 8 Visitor Access Records

viii. NIST SP 800-53 Revision 4: PE 9 Power Equipment and Cabling

ix. NIST SP 800-53 Revision 4: PE 10 Emergency Shutoff

x. NIST SP 800-53 Revision 4: PE 11 Emergency Power

xi. NIST SP 800-53 Revision 4: PE 13 Fire Protection

xii. NIST SP 800-53 Revision 4: PE 14 Temperature and Humidity Controls

xiii. NIST SP 800-53 Revision 4: PE 15 Water Damage Protection

xiv. NIST SP 800-53 Revision 4: PE 16 Delivery and Removal

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

APPENDIX K

Information Security - Risk Management

1. Risk Management

a. Risk management typically consists of the following:

i. Risk Assessment: A risk assessment is the first process of risk management and is used to determine the extent of the potential threat and the risk associated with IT security.

ii. Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls for the risks identified during the risk assessment process.

b. Risk Management Strategy (PM 9)

i. DDSN shall define a schedule for an on-going risk assessment and risk mitigation process.

ii. DDSN shall review and evaluate risk based on the system categorization level and/or data classification of their systems.

c. Guidance:

i. NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy

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

2. Risk Assessment

a. Policy Risk Assessment (RA 3)

i. The DDSN shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards. This assessment framework shall clearly define accountability, roles, and responsibilities.

b. Security Assessment (CA 2)

i. DDSN shall annually conduct a formal assessment of the IT security processes and controls to determine the appropriateness of the design and implementation of controls, and the extent to which the controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for their systems.

ii. DDSN shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the DDSN.

c. Plan of Action and Milestones (CA 5)

i. DDSN shall develop and periodically update a Plan of Action and Milestones (POAM) document that shall identify any deficiencies related to internal security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments.

ii. DDSN shall develop and periodically update a Corrective Action Plan (CAP) to identify activities planned or completed to correct deficiencies identified during the security assessment review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known risks in DDSN systems.

d. Security Authorization (CA 6)

i. DDSN shall establish a process and assign a senior level executive or manager to determine whether or not risks can be accepted, and for each of the risks identified following the risk assessment, the designated personnel within the DDSN shall make a decision regarding risk treatment.

e. Continuous Monitoring (CA 7)

i. DDSN shall continuously monitor the security controls within its information systems to ensure that the controls are operating as intended.

f. Guidance:

i. NIST SP 800-15
ii. NIST SP 800-53 Revision 4: RA 3 Risk Assessment
iii. NIST SP 800-53 Revision 4: CA 2 Security Assessment
iv. NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones
v. NIST SP 800-53 Revision 4: CA 6 Security Authorization
vi. NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

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

3. Risk Mitigation

a. Continuous Monitoring (CA 7)

i. DDSN shall establish and implement controls to ensure risks are reduced to an acceptable level based on security requirements and once threats have been identified and decisions for the management of risks have been made.

ii. DDSN shall determine and document the acceptable level for risk for various threats based on the business requirements and the impact of the potential risk to the [Agency].

b. Guidance:

i. NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

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

APPENDIX L

Information Security - Threat and Vulnerability Management

1. Vulnerability Assessment

   a. Vulnerability Scanning (RA 5)

      i. DDSN shall implement processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems / applications are reported.

      ii. DDSN shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports.

      iii. DDSN shall analyze vulnerability scan reports and results from security control assessments.

      iv. DDSN shall remediate identified vulnerabilities in accordance with DDSN assessment of risk.

   b. Penetration Testing (CA 8)

      i. DDSN shall conduct penetration testing exercises on an annual basis, either by use of internal resources or employing an independent third-party penetration team.

   c. Guidance:

      i. NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
      ii. NIST SP 800-53 Revision 4: CA 8 Penetration Testing

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

2. Incident Management

   a. Incident Response Policy and Procedures (IR 1)

      i. DDSN shall develop, document, and publish an incident response policy that addresses scope, roles, and responsibilities, internal coordination efforts, and compliance.

      ii. DDSN shall establish formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.

iii. DDSN shall review and update the incident response policy and procedures on an annual basis.

b. Incident Response Plan (IR 8)

i. DDSN shall develop and/or hire a third-party vendor to implement an incident response plan to:

1. Establish a roadmap for implementing incident response capabilities;
2. Identifies and documents the requirements of the organization, including mission, size, structure, and functions;
3. Define the types of information security incidents to be reported;
4. Establish metrics to help ensure incident response capabilities remain effective; and
5. Define resources, such as technology and personnel, required to effectively support incident response capabilities.

ii. DDSN shall review and update the incident response plan on an annual basis.

c. Incident Handling (IR 4)

i. DDSN shall implement formal processes to manage security incidents, including preparation, detection and analysis, containment, eradication, and recovery.

ii. DDSN shall implement dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents.

d. Incident Monitoring and Reporting (IR 5, IR 6)

i. DDSN shall establish a process and tools to maintain detailed records of information security incidents that occur in external (e.g., boundary systems) and internal information systems.

ii. DDSN shall implement a policy to require personnel to report suspected information security incidents to the incident response team and/or DDSN leadership.

e. Information System Monitoring (SI 4)

i. DDSN shall monitor information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.

ii. DDSN shall deploy monitoring devices strategically within information technology environment to collect information security events and associated information.

iii. DDSN shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.

iv. DDSN shall monitor inbound and outbound communications traffic to/ from the information system for unusual or unauthorized activities or conditions.

v. DDSN shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to DDSN operations, individuals, and assets,

f. Incident Response Training (IR 2)

i. DDSN shall provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.

ii. DDSN shall provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

g. Incident Response Testing (IR 3)

i. DDSN shall establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.

ii. DDSN shall document the incident response test results and update incident response processes as applicable.

h. Malicious Code Protection (SI 3)

i. DDSN shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.

ii. DDSN shall implement a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.

iii. DDSN shall configure malicious code protection mechanisms to perform periodic scans at defined time intervals.

iv. DDSN shall block malicious code and send an alert to information system/networks administrator and initiate action(s) in response to malicious code detection.

i. Guidance

i. NIST SP 800-53 Revision 4: IR 1 Incident Response Policy and Procedures
ii. NIST SP 800-53 Revision 4: IR 2 Incident Response Training
iii. NIST SP 800-53 Revision 4: IR 3 Incident Response Testing
iv. NIST SP 800-53 Revision 4: IR 4 Incident Handling
v. NIST SP 800-53 Revision 4: IR 5 Incident Monitoring
vi. NIST SP 800-53 Revision 4: IR 6 Incident Reporting
vii. NIST SP 800-53 Revision 4: IR 8 Incident Response Plan
viii. NIST SP 800-53 Revision 4: SI 3 Malicious Code Protection
ix. NIST SP 800-53 Revision 4: SI 4 Information System Monitoring

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

3. Patch Management

a. Flaw Remediation (SI 2)

i. DDSN shall develop and implement a process to identify, report, and correct information system flaws.

ii. DDSN shall establish a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.

iii. DDSN shall install latest stable versions of applicable security software and firmware updates.

iv. DDSN shall establish a patch cycle that guides the normal application of patches and updates to systems.

v. DDSN shall establish a process of patch testing to verify the source and integrity of the patch and ensure testing in a production mirrored environment for a smooth and predictable patch roll out.

b. Guidance:

i. NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
ii. NIST SP 800-53 Revision 4: CM 2 Baseline Configuration

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

APPENDIX M

Data Protection and Privacy

1. Data Classification

   a. Security Categorization (RA 2)

      i. 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 negligible 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.

      ii. 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.

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

b. Guidance

i. NIST SP 800-53 Revision 4: RA 2 Security Categorization

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

2. Data Disposal

a. Policy Media Sanitization (MP 6)

i. 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.

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

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

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

v. 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.

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

vii. 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.

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

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

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

b. Guidance:

i. NIST SP 800-53 Revision 4: MP 6 Media Sanitization

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

3. Data Protection

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

i. 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.

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

b. Cryptographic Key Establishment and Management (SC 12)

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

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

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

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

c. Cryptographic Protection (SC 17)

i. 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.

ii. 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.

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

d. Transmission Confidentiality and Integrity (SC 8 and SC 9)

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

ii. 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).

iii. 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.

iv. 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.

e. Guidance:

i. NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures
ii. NIST SP 800-53 Revision 4: SC 8 Transmission Integrity
iii. NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality
iv. NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management
v. NIST SP 800-53 Revision 4: SC17 Cryptographic Protection

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

4. Privacy

a. Policy Privacy Impact Assessment

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

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

iii. 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).

iv. PIAs shall include:

1. What information is to be collected (e.g., nature and source).
2. Why information is being collected (e.g., to determine eligibility).
3. Intended use of information (e.g., to verify existing data).
4. With whom the information will be shared.
5. What opportunities individuals have to decline to provide information.
6. How the information will be secured.

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

vi. 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.

vii. 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.

b. Guidance:

i. Fair Information Practice Principles (FIPPs)
ii. OMB Memorandum 03-22

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

APPENDIX N

Acceptable Use of Network Services and the Internet

1. General Principles

   a. Access to computer systems and networks owned or operated by DDSN and the State of South Carolina imposes certain responsibilities and obligations on state employees and officials (hereinafter termed "users") and is subject to state government and DDSN policies and local, state and federal laws. Acceptable use always is ethical, reflects honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of information, system security mechanisms, and the individual's rights to privacy and freedom from intimidation, harassment, and unwarranted annoyance.

   b. Regardless of the physical location of the User's workplace (e.g., telecommuting), the User is subject to the requirements of this directive.

   c. Users may be required to comply with supplemental requirements imposed for specific information systems.

   d. DDSN may inspect and/or seize any DDSN-issued device and/or data stored on any DDSN-issued information system and/or device. User acknowledges that he/she has no expectation of privacy as to any communication and/or information stored within any DDSN-issued information system or device, whether or not that information is stored locally, on a hard drive, or on other media in use with the unit.

   e. For network maintenance and security purposes, all DDSN information systems are subject to monitoring and interception of information. User acknowledges that DDSN may monitor and intercept User's communications on DDSN information systems for purposes including, but not limited to, system testing, security, investigations of alleged personnel misconduct, and/or law enforcement investigations.

   f. Users who violate any copyright declarations are acting outside the course and scope of their employment with DDSN or other authority and the State of South Carolina is relieved of any legal responsibility. Users will be personally responsible and liable for such infringing activities.

   g. By participating in the use of networks and systems provided by DDSN and the State of South Carolina, users agree to be subject to and abide by this policy for their use. Willful violation of the principles and provisions of this policy may result in disciplinary action up to and including termination.

h. In accordance with DDSN Directive 367-17-DD: Human Resource and Security Awareness Policy, employees, contractors, and third-party users shall agree and sign this policy.

i. User will complete DDSN privacy and security training prior to accessing any non-public data and/or DDSN information systems, and User will complete privacy and security training on an annual basis thereafter. User shall not take software home for personal use on a home computer.

j. This document may be updated on an as-needed basis and is subject to annual review.

2. Specific Provisions

a. Users shall:

i. Agree that DDSN-issued devices and systems are the property of the DDSN and will be used only for DDSN authorized purposes, except that incidental use of DDSN resources/property is permitted as long as it does not result in additional public expense. Incidental use is infrequent and minimal. Unauthorized use of, or access to, a DDSN-issued device or systems is prohibited and may subject the user to employee discipline and/or legal actions.

ii. Refrain from monopolizing systems, overloading networks with excessive data or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.

iii. User will neither share his/her DDSN-issued User ID and/or password with any other person, nor knowingly allow any other person to use his/her User ID and/or password. If User suspects his/her password has been compromised, he/she will inform DDSN Information Technology Department and/or DDSN's Information Security Officer immediately.

iv. Assume personal responsibility for any charges associated with billable services unless appropriate authorization has been obtained.

v. At termination of employment, User will not remove from DDSN any information, hardware, software, device, or any other workplace resource, without explicit written permission from DDSN executive management; and

vi. At termination of employment, User will return all DDSN information, hardware, software, device, or any other workplace resource to User's supervisor.

b. Users shall not:

i. Use the DDSN-issued devices and systems for private purposes, including blogging, commenting or posting on social media, sharing photographs, or other non-work related purposes, without written permission from DDSN executive management including illegal, unlawful, immoral purposes or to support or assist such purposes. Examples of this would be the transmission of violent, threatening, defrauding, obscene or otherwise illegal or unlawful materials.

NOTE: It is advised that no DDSN business, consumer data or other DDSN-related information be shared to employees' personal social media pages. Please refer to DDSN Directive 413-04-DD: Social Media Usage, regarding how DDSN expects employees to use social media from a personal perspective.

ii. Use mail or messaging services to harass, intimidate or otherwise annoy another individual.

iii. Use the networks or other state equipment for private, recreational, non-public purposes including the conduct of personal commercial transactions.

iv. Use the networks or other state equipment for commercial or partisan political purposes.

v. Use the networks or other state equipment for personal gain such as selling access to a USER ID or by performing work for profit with state resources in a manner not authorized by the State.

vi. Use the network to disrupt network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, propagation of computer "worms" and viruses, and sustained high volume network traffic which hinders others in their use of the network.

vii. Attempt to circumvent or subvert system or network security measures.

viii. Intercept network traffic for any purpose unless engaged in authorized network administrative duties.

ix. Make or use illegal copies of copyrighted software or other mediums, store such copies on state systems, or transmit them over state networks.

x. Store or back-up any DDSN non-public information to any non-DDSN information system or device such as portable hard drives

Acceptable Use of Network Services and the Internet

South Carolina Department of Disabilities and Special Needs

- I acknowledge that I have received a copy of the Acceptable Use of Network Services and the Internet policy.

- I acknowledge that I have read and understand the Acceptable Use of Network Services and the Internet policy.

- I authorize the Department of Disabilities and Special Needs (DDSN) staff to monitor any communications to or from myself on the DDSN network and internet.

- I understand that any violation of the provisions in the Acceptable Use of Network Services and the Internet policy is subject to the disciplinary action in accordance with DDSN's progressive disciplinary policy, and/or possible legal action.

- I agree to abide by DDSN's Acceptable Use of Network Services and the Internet policy.

______________________________ ______________________________
User Name (Printed) User Signature

Date:__________________________

APPENDIX O

Service Provider Data Protection

1. Purpose

   a. Assure that each DSN Board/Provider assigns the responsibility for data security to a specific individual to provide organizational focus and importance to security, privacy and that the assignment of responsibility is documented.

   b. Responsibilities include:

      i. The management and supervision of the use of security measures to protect data, and

      ii. The management and conduct of all personnel in relation to that data. This includes the notification of all additions, changes, or deletions of any user of DDSN information systems.

2. Statement

   a. It is the policy of the South Carolina Department of Disabilities and Special Needs (DDSN) to have one official designated by each DSN Board/Provider as the Data Security Administrator who is responsible for the implementation of the required policies and procedures.

3. Standards

   a. Assigned Security Responsibility – Policy Standards

      i. Each DSN Board/Provider shall designate at least one (1) individual as the Data Security Administrator to coordinate data security and data privacy activities in conjunction with the DDSN Information Security Officer and/or Data Privacy Officer.

         1. The assignment of responsibility of the Data Security Administrator shall include the development and implementation of policies and procedures to safeguard electronic protected/confidential or restricted information within organizational requirements.
         2. The assignment of responsibility of the Data Security Administrator shall include the supervision over the conduct of all personnel in relation to the protection of electronic protected, confidential, or restricted information.
         3. The assignment and designation of the Data Security Administrator shall be documented.

b. Assigned Security Responsibility - Procedural Standards

i. Each DSN Board/Provider shall have an individual designated for security responsibilities that will coordinate security activities locally.

ii. Each DSN Board/Provider's designated security administrator shall be responsible for ensuring all DDSN security procedures are followed by issuing and terminating DDSN security privileges.

iii. The Data Security Administrator shall be responsible for oversight of the conduct of personnel in the protection of the data locally at each DSN Board/Provider.