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

SOUTH CAROLINA Department OF Disabilities AND Special Needs

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

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

Reference Number:	367-18-DD
Title of Document:	Information Security Policy - Access Control
Date of Issue:	October 5, 2015
Effective Date:	October 5, 2015
Last Review Date:	October 5, 2015
Date of Last Revision:	July 13, 2016 **(NEW)**
Applicability:	All DDSN Employees

I. ACCESS MANAGEMENT

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.

Access Control Policy and Procedures (AC 1)

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

Account Management (AC 2)

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

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

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

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.

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.

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

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.

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

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

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.

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

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

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

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

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

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

Access Enforcement (AC 3)

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

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

Information Flow Enforcement (AC 4)

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.

Separation of Duties (AC 5)

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

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

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

Least Privilege (AC 6)

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."

DDSN shall implement processes or mechanisms to:

- Disable file system access not explicitly required for system, application, and administrator responsibilities;
- Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;
- Restrict use of database management to authorized database administrators;

- Grant access to authorized users based on their required job duties; and

- Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.

Unsuccessful Login Attempts (AC 7)

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.

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.

System Use Notification (AC 8)

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."

Session Lock (AC 11)

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

Guidance: *NIST SP 800-53 Revision 4: AC 1 Access Control Policy And Procedures*
NIST SP 800-53 Revision 4: AC 3 Access Enforcement
NIST SP 800-53 Revision 4: AC 4 Information Flow Enforcement
NIST SP 800-53 Revision 4: AC 5 Separation Of Duties
NIST SP 800-53 Revision 4: AC-6 Least Privilege
NIST SP 800-53 Revision 4: AC 7 Unsuccessful Login Attempts
NIST SP 800-53 Revision 4: AC 8 System Use Notification
NIST SP 800-53 Revision 4: AC 11 Session Lock

NETWORK ACCESS MANAGEMENT

The purpose of the network access management section is to establish procedures to control and monitor access and use of the network infrastructure. These are necessary to preserve the integrity, availability and confidentiality of DDSN information. Users of these services are therefore advised of this potential monitoring and agree to this practice.

Remote Access (AC 17)

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

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

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

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.

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.

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).

Wireless Access (AC 18)

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

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

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

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

Use of External Information Systems (AC 20)

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.

Boundary Protection (SC 7)

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

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.

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

Guidance: *NIST SP 800-53 Revision 4: AC 17 Remote Access*
NIST SP 800-53 Revision 4: AC 18 Wireless Access
NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
NIST SP 800-53 Revision 4: SC 7 Boundary Protection

IDENTITY MANAGEMENT

The purpose of the identity management section is to establish a standardized method to create and maintain verifiable user identifiers, and enable decisions about the levels of access to be given to each individual and/or groups.

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

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.

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

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.

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).

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.

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

Guidance: *NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)*
NIST SP 800-53 Revision 4: IA 4 Identifier Management
NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)

AUTHENTICATION

The purpose of the authentication section is to establish the authentication methods utilized by the DDSN for authenticating, external/remote access connections, VPN access, administrative function access, vendor access and remote access to sensitive information.

Authenticator Management (IA 5)

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

Unsuccessful Logon Attempts (AC 7)

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

Session Lock (AC 11)

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

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

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

Guidance: *NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts*
NIST SP 800-53 Revision 4: AC 11 Session Lock
NIST SP 800-53 Revision 4: IA 5 Authenticator Management

EMERGENCY ACCESS

The purpose of the emergency access section is to establish conditions under which emergency access is granted, outlines rules to determine who is eligible to obtain emergency access and the authorized personnel entitled to grant access.

Policy Account Management (AC 2)

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

The emergency procedures shall ensure that:

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

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.

Guidance: *NIST SP 800-53 Revision 4: AC 2 Account Management*

PASSWORD POLICY

The purpose of the password policy section is to establish uniform and enterprise-wide practices to create, manage and maintain passwords to ensure expected level of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

Account Management (AC 2)

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

- Automatically force users (including administrators) to change user account passwords every 90 days.
- Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every 60 days;
- Passwords for system accounts to be changed at least every one hundred 180 days;
- Enforce password minimum lifetime of one (1) day;
- Prohibit the use of dictionary names or words as passwords;
- Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters;
- 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.
- Encrypt passwords in storage and during transmission;
- Prohibit password reuse for six (6) generations prior to reuse;

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

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

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.).

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

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

Guidance: *NIST SP 800-53 Revision 4: AC 2 Account Management*

PASSWORD ADMINISTRATION

The purpose of the password administration section is to ensure that the allocation of passwords is controlled through a formal management process.

Policy Access Agreements (PS 6)

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.

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

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

DDSN shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password.
DDSN shall establish a process to uniquely identify and authenticates non-Agency users.

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

Authenticator Management (IA 5)

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

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.

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

Authenticator Feedback (IA 6)

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

Guidance: *NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)*
NIST SP 800-53 Revision 4: IA 5 Authenticator Management
NIST SP 800-53 Revision 4: IA 6 Authenticator Feedback
NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)
NIST SP 800-53 Revision 4: PS 6 Access Agreements

IMPLEMENTATION, MAINTENANCE, AND COMPLIANCE

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

Any revisions to this policy shall be developed by the Information Security Officer and follow the normal approval process for DDSN directives.

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

Tom Waring
Associate State Director-Administration
(Originator)

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

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