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:	367-23-DD
Title of Document:	Information Security Policy - Information Systems Acquisitions, Development, and Maintenance
Date of Issue:	May 3, 2016
Effective Date:	May 3, 2016
Date of Last Revision:	July 13, 2016
Applicability:	All DDSN Employees **(REVISED)**

---

1. Change Management

The purpose of the change management is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner to production, and applicable non-production environments with minimal impact and risk.

Configuration Change Control (CM 3)

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

- All requests for change shall be handled in a structured way that determines the impact on the operational system and its functionality;
- All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner.

- DDSN shall have a process to categorize, prioritize and authorize changes to information systems;

- Post-implementation reviews shall be performed to ensure production changes are operating as intended;

- A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;

- A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; and

- Information systems shall be reviewed and tested after major changes to operating systems.

Guidance: *NIST SP 800-53 Revision 4: CM 3 Configuration Change Control*

2. Configuration Management

The purpose of the configuration management is to establish procedures for the compliance with minimally acceptable system configuration requirements, as determined by DDSN. In addition, this section helps ensure DDSN establish processes to identify and implement secure configurations, control configuration changes, and monitor security controls to validate adherence with approved configurations.

Policy Baseline Configuration (CM 2)

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

- 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.

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

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

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

Configuration Management Plan (CM 9)

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

Guidance *NIST SP 800-53 Revision 4: CM 2 Baseline Configuration*
NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan
NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems

3. System Development and Maintenance

The purpose of system development and maintenance is to define requirements for system security planning and to improve protection of DDSN information system resources.

Policy System Security Plan (PL 2)

- DDSN shall prepare system security plans and documentation for critical enterprise information systems or systems under development.
- 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.
- When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

Vulnerability Scanning (RA 5)

- DDSN shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.
- DDSN shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.
- Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.
- System and Services Acquisition Policy and Procedures (SA 2)
- 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.
- DDSN shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

System Development Life Cycle (SA 3)

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

External Information System Services (SA 9)

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

Developer Security Testing and Evaluation (SA-11)

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

Flaw Remediation (SI 2)

- DDSN shall design appropriate controls into information systems, including user developed applications to ensure correct processing.
- DDSN shall ensure that software patches are applied when they function to remove or reduce security weaknesses.

Security Alerts, Advisories, and Directives (SI 5)

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

Software, Firmware, and Information Integrity (SI 7)

- 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).
- 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.

Information Input Validation (SI 10)

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

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

Session Authenticity (SC 23)

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

Policy Supplement	*Threat and Vulnerability Management 1.1: Patch Management* *Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution*
Guidance:	*NIST SP 800-53 Revision 4: PL 2 System Security Plan* *NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning* *NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure* *NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle* *NIST SP 800-53 Revision 4: SA 9 External Information System Services* *NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation* *NIST SP 800-53 Revision 4: SI 2 Flaw Remediation* *NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity* *NIST SP 800-53 Revision 4: SI 10 Information Input Validation* *NIST SP 800-53 Revision 4: SC 23 Session Authenticity*

4. Release Management

The purpose of release management is to define the appropriate release activities during an implementation or upgrade of information systems.

Policy Allocation of Resources (SA 2)

- 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).

- DDSN shall determine as part of the release planning process:

    - Resources required to deploy the release;
    - Pass/fail criteria;
    - Build and test plans prior to implementation;
    - Pilot and deployment plans; and
    - Develop requirements for the release.

Information System Documentation (SA 5)

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

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

Security Engineering Principles (SA 8)

- DDSN shall implement standardization and enforce operational controls through the use of change requests for deploying releases into production.

Guidance: *NIST SP 800-53 Revision 4: SA 2 Allocation of Resources*
NIST SP 800-53 Revision 4: SA 5 Information System Documentation
NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles

Tom Waring
Associate State Director-Administration
(Originator)

Beverly A.H. Baseemi, 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