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

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

Reference Number:	367-26-DD
Title of Document:	Information Security Policy – Risk Management
Date of Issue:	June 1, 2016
Effective Date:	June 1, 2016
Last Review Date:	June 1, 2016
Date of Last Revision:	June 1, 2016
Applicability:	All DDSN Employees **(NEW)**

PURPOSE

The purpose of the risk management policy is to define the processes and controls that shall be implemented by DDSN to identify, assess, and manage information security risks to an acceptable level. DDSN shall ensure ongoing compliance with applicable Federal and State laws and regulations.

I. RISK MANAGEMENT

Risk management typically consists of the following:

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

Risk Management Strategy (PM 9)

DDSN shall define a schedule for an on-going risk assessment and risk mitigation process. DDSN shall review and evaluate risk based on the system categorization level and/or data classification of their systems.

Guidance: *NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy*

II. RISK ASSESSMENT

Policy Risk Assessment (RA 3)

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.

Security Assessment (CA 2)

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.

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

Plan of Action and Milestones (CA 5)

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.

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.

Security Authorization (CA 6)

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.

Continuous Monitoring (CA 7)

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

Guidance: *NIST SP 800-15*
NIST SP 800-53 Revision 4: RA 3 Risk Assessment
NIST SP 800-53 Revision 4: CA 2 Security Assessment
NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones
NIST SP 800-53 Revision 4: CA 6 Security Authorization
NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring

III. RISK MITIGATION

Continuous Monitoring (CA 7)

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.

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].

Guidance: *NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring*

Tom Waring
Associate State Director-Administration
(Originator)

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

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