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

Reference Number:	367-29-DD
Title of Document:	Information Security Program Master Policy
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 this Master Policy is to establish the principles to regulate how DDSN shall provide an appropriate level of governance controls over Information Security related activities. DDSN shall establish key principles based on which DDSN's Security Organization shall be established. DDSN shall establish key principles based on which DDSN's security procedures and controls shall be developed and deployed.

I. INFORMATION SECURITY PROGRAM PLANNING

Information Security Plan (PM 1)

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.

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.

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

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

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

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

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

Information Security Resources (PM 3)

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

Plan of Action and Milestones Process (PM 4)

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.

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

Information Security Measures of Performance (PM 6)

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 (SC DIS) and the South Carolina Enterprise Privacy Office (SC EPO).

Guidance: *NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan*
NIST SP 800-53 Revision 4: PM 3 Information Security Resources
NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process
NIST SP 800-53 Revision 4: PM 6 Measures of Performance

II. SECURITY ORGANIZATION (ROLES and RESPONSIBILITIES)

Information Security Authority (2.2.3.1)

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.

Information Security Liaison (PM 2)

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

Information Security Workforce (PM 13)

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

Role-based Security Training (AT 3)

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

Guidance: *NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer*
NIST SP 800-53 Revision 4: PM 13 Information Security Workforce
NIST SP 800-53 Revision 4: AT 3 Role-based Security Training
NIST SP 800-100: 2.2.3.1 Agency Head

III. POLICY MANAGEMENT (PLAN OF ACTION)

Procedure Development

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.

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

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.

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.

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

- Revision history
- Introduction
- Preface
- Ownership, roles, and responsibilities

- Purpose
- Policy statements
- Policy supplement
- Guidance
- Definitions

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

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

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

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.

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

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

Procedure Review and Approval

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

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

Procedure approval history shall be documented in detail.

Procedure Implementation

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.

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

Guidance: *NIST SP 800-53 Revision 4: PM 6 Measures of Performance*

IV. INFORMATION SECURITY CONTROLS DEPLOYMENT

Controls Deployment

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

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

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.

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.

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

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.

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

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

DEFINITIONS

Agency, State Government: Refers to any South Carolina state agency, institution, department, division, board, commission, or authority.

Control, Information Security: Refers to any process or technology intended to reduce a security risk.

Guidance: Guidance refers to best practices and industry standards that have been used as a guide to develop the security policies and the policy supplements.

Information Security Liaison: Official responsible for carrying out the "Chief Information Officer" responsibilities within the agency under the Federal Information Security Management Act (FISMA) and serving as the primary liaison between the DIS office of the Chief Information Security Officer and the agency's authorizing officials, information system owners, and information system security officers.

Information Security Plan: The collection of procedures and other guidance developed by state government agencies to implement the SC DIS Information Security Program within the agency.

Metrics: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Policy: The Information Security Policy defines appropriate controls to protect an agency's information assets from unauthorized disclosure, misuse, alteration, or destruction in a manner that ensures compliance with regulatory requirements and risk management expectations.

Policy supplement: Policy supplement assists the agencies in the actual implementation of the high level security controls defined in the policy. This defines at a granular level the baseline security controls for the agency.

Policy exemptions: Scenarios which require exemption from the existing provisions of the Security policy are called policy exemptions.

Risk posture: Risk posture identifies the specific threats that the agency faces and quantifies the risks associated with each of those threat events materializing.

SC DIS: South Carolina Division of Information Security.

SC DIS Information Security Program: The collection of policies, procedures, and other guidance published on the SC DIS website (dis.sc.gov).

Standards: Security baseline to assist agencies, used to maintain a minimum baseline security configuration level as per industry guidelines.

System Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

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