SOUTH CAROLINA DIVISION OF INFORMATION SECURITY (SC DIS)

Information Security Program

Master Policy

V1.2 – June 13, 2014

Revision History

Date	Authored by	Title	Ver.	Notes
07-Mar-2104	Division of Information Security	Governance	1.0	Initial draft.
25-Mar-2014	Division of Information Security	Master Policy	1.1	Establish implementation timeline; refine titles and duties. Add Controls Deployment section.
13-June-2014	Division of Information Security	Master Policy	1.2	Established implementation timeline for Information Security Controls Deployment.

Table of Contents

INTRODUCTION

Part 1. Preface

The South Carolina Information Security (Infosec) Program consists of information security policies, procedures, and other guidance that establish a common information security framework across South Carolina State Government Agencies.

Together these policies provide a framework for developing a state government agency's information security plan. An effective information security plan improves the State's security posture and aligns information security with an agency's mission, goals, and objectives.

Each agency's implementation of the Infosec Program must comply with the policy framework established by the SC DIS, as published in the *Policies* section of its website: http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx.

Part 2. Organizational and Functional Responsibilities

This section sets the minimum level of responsibility for the following individuals and/or groups:

- Division of Information Security
- State Government Agencies
- Employees, Contractors, and Third Parties

(A) Division of Information Security

The duties of the Division of Information Security are:

- Developing, maintaining, and revising information security policies, procedures, and recommended technology solutions
- Providing technical assistance, advice, and recommendations concerning information security matters
- Coordinating information security incident response for any incidents involving state government agencies

(B) State Government Agencies

Information security is a state government agency's responsibility shared by all members of the agency's management team. The management team shall provide clear direction and visible support for security initiatives. Each agency is responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy
- Implementing and maintaining an Information Security Plan compliant with the SC DIS Information Security Program
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency's information security plan
- Ensuring that security is part of the information systems planning and procurement process
- Participating in annual information systems data security self-audits ensuring that the agency's own practices are in compliance with the agency's Information Security Plan, and with the SC DIS Information Security Program

- Determining the feasibility of conducting regular external and internal vulnerability assessments and penetration testing to verify security controls are working properly and to identify weaknesses
- Implementing a risk management process for the life cycle of each critical information system
- Assuring the confidentiality, integrity, availability, and accountability of all of the agency's information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with those processing functions
- Ensuring that agency staff work with SC DIS and/or SC Enterprise Privacy Office (EPO) staff in resolving the agency's security and privacy incidents
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for the agency's system users
- Identifying 'business owners' for any new system, who are responsible for:
    - Classifying data according to the criteria published by SC DIS or SC EPO
    - Approving access and permissions to the data
    - Ensuring methods are in place to prevent and monitor inappropriate access to confidential data
    - Determining when to retire or purge the data

(C) Employees, Contractors and Third Parties

All State employees, contractors, and third party personnel are:

- Responsible for being aware of and complying with statewide and internal policies and their responsibilities for protecting IT assets of their agency and the State
- Responsible for using information resources only for intended purposes as defined by policies, laws and regulations of the State or agency
- Accountable for their actions relating to their use of all State information systems

Part 3. Section Overview

Each information security policy section consists of the following:

- **Purpose:** Provides background to each area of the information security policies.
- **Policy:** Contains detailed policies that relate to each information security section, and relations with National Institute of Standards and Technology (NIST) Special Publications (SP) 800-53 Revision 4 controls.
- **Policy Supplement:** Contains the security solution recommendations that are connected to the South Carolina Information Security Recommended Technology Solutions.
- **Guidance:** Provides references to guidelines on information security policies.
- **Reference:** Provides a reference to the guidance in the form of a uniform resource locator (URL).

Part 4. Implementation Timeline

Each state government agency should observe the following timeline in implementation of the Information Security Program. Exceptions must be reported to the office of the SC DIS Chief Information Security Officer.

Section	Implementation Date
1.1 Information Security Program Planning	30-Jun-2014
1.2 Security Organization (Roles and Responsibilities)	30-Jun-2014
1.3 Policy Management (Plan of Action)	31-Jan-2015
1.4 Information Security Controls Deployment	1-July-2016

INFORMATION SECURITY POLICY

Governance

1.1 Information Security Program Planning

Purpose

The purpose of this section is to establish the principles to regulate how agencies shall provide an appropriate level of governance controls over Information Security related activities.

Policy

Information Security Plan (PM 1)

- Each agency 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.
- Each agency'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.
- Each agency shall ensure coordination among the agency's business units responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.)
- Each agency shall ensure that the security plan is approved by senior management.
- Each agency shall review the information security plan at least on an annual basis.
- Each agency shall update the security plan to address changes and problems identified during plan implementation or security control assessments.
- Each agency shall protect the information security plan from unauthorized disclosure and modification.

Information Security Resources (PM 3)

- Each agency 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)

- Each agency shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.
- Each agency 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)

- Each agency shall develop, monitor, and report on the results of information security measures of performance, as directed or

	guided by the SC DIS and SC EPO.
Policy Supplement	A policy supplement has not been identified.
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
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Security Organization (Roles and Responsibilities)

Purpose

The purpose of this section is to establish key principles based on which each Agency's Security Organization shall be established.

Policy

Information Security Authority (2.2.3.1)

- Each agency'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)

- Each agency 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)

- Each agency 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)

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

Policy Supplement

A policy supplement has not been identified.

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

Reference

http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx
http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf

1.3 Policy Management (Plan of Action)

Purpose

The purpose of this section is to establish key principles based on which each agency's security procedures shall be developed.

Policy

Procedure Development

- Each agency shall adopt a risk-based approach to identify State and agency-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.
- Each agency shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.
- Each agency 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.
- Each agency 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.
- Each agency shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.

- Each agency 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.
- Each agency shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.
- Each agency 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

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

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PM 6 Measures of Performance
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Information Security Controls Deployment

Purpose

The purpose of this section is to establish key principles for deployment of information security controls.

Policy

Controls Deployment

- Each agency shall adopt a risk-based approach to prioritize deployment of controls.
- Each agency shall allocate the appropriate subject matter experts to the deployment of State and agency-specific information security controls.
- Each agency 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.
- Each agency shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective.
- Each agency 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.
- Each agency shall develop and implement a communication plan to disseminate new controls or changes to existing controls.
- Each agency shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.

Policy Supplement

A policy supplement has not been identified.

Guidance

Guidance has not been identified.

Reference

http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

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.