

# **DIVISION OF INFORMATION SECURITY (DIS)**

---

## **Information Security Policy – Governance**

Draft V0.1 – March 7, 2014

## Revision History

---

Update this table every time a new edition of the document is published

<b>Date</b>	<b>Authored by</b>	<b>Title</b>	<b>Ver.</b>	<b>Notes</b>
3/07/2014	Division of Information Security	Governance	1.0	Initial draft

DRAFT

## Table of Contents

---

<b>INTRODUCTION .....</b>	<b>3</b>
PART 1. PREFACE .....	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES .....	3
PART 3. PURPOSE .....	4
PART 4. SECTION OVERVIEW .....	4
<b>INFORMATION SECURITY POLICY .....</b>	<b>5</b>
<i>Governance</i> .....	5
1.1 <i>Information Security Program Planning</i> .....	5
1.2 <i>Security Organization (Roles and Responsibilities)</i> .....	7
1.3 <i>Information Security Policy Management</i> .....	8
<b>DEFINITIONS .....</b>	<b>10</b>

DRAFT

## INTRODUCTION

---

### Part 1. Preface

The South Carolina Information Security (INFOSEC) Program consists of information security policies that establish a common information security framework across South Carolina State Government Agencies and Institutions.

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

### Part 2. Organizational and Functional Responsibilities

The policy sets the minimum level of responsibility for the following individuals and/or groups:

- Division of Information Security
- Agency/Institution
- 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

#### (B) Agency/Institution

Information security is an agency/institution responsibility shared by all members of the State agency/institution management team. The management team shall provide clear direction and visible support for security initiatives. Each agency/institution is responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy
- Implementing and maintaining an Information Security Program
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency security program
- Ensuring that security is part of the information planning and procurement process
- Participating in annual information systems data security self-audits focusing on compliance to this State data security policy
- 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 agency information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with those processing functions
- Assuming the lead role in resolving agency security and privacy incidents

- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for agency system users
- Identifying ‘business owners’ for any new system that are responsible for:
  - Classifying data
  - 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
- Using information resources only for intended purposes as defined by policies, laws and regulations of the State or agency
- Being accountable for their actions relating to their use of all State information systems

## **Part 3. Purpose**

The information security policies set forth the minimum requirements that are used to govern the South Carolina Information Security (INFOSEC) Program. Agencies and institutions are expected to comply with the State’s information security policies. Agencies and institutions may leverage existing policies or develop policies based on the guidance from the State’s information security policies. These policies exist in addition to all other [Agency] policies and federal and State regulations governing the protection of [Agency] data. Adherence to the policies shall improve the security posture of the State and help safeguard [Agency] information technology resources.

## **Part 4. 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).

## INFORMATION SECURITY POLICY

---

### Governance

---

#### 1.1 Information Security Program Planning

Purpose	The purpose of the Information Security Program Planning section is to establish the principles to regulate how [Agency] shall provide an appropriate level of governance controls over Information Security related activities.
Policy	<p>Information Security Program Plan (PM 1)</p> <ul style="list-style-type: none"><li>• [Agency] shall develop and communicate an agency-wide information security program plan that underlines security requirements, the security program management controls, and common controls in place for meeting those requirements.</li><li>• [Agency] security plan shall identify and assign of security program roles, responsibilities and management commitment, and ensure coordination among agency entities, and compliance to the security program/ plan.</li><li>• [Agency] shall ensure coordination among agency entities responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.)</li><li>• [Agency] shall ensure that the security plan is approved by senior management.</li><li>• [Agency] shall review the agency-wide information security program plan at least on an annual basis.</li><li>• [Agency] shall update the security plan to address changes and problems identified during plan implementation or security control assessments.</li><li>• [Agency] shall protect the information security program plan from unauthorized disclosure and modification.</li></ul> <p>Information Security Resources (PM 3)</p> <ul style="list-style-type: none"><li>• [Agency] shall consider resources needed to implement and maintain the information security program in capital planning and investment requests.</li></ul> <p>Plan of Action and Milestones Process (PM 4)</p> <ul style="list-style-type: none"><li>• [Agency] shall implement a process for ensuring that plans of action and milestones for the security program and associated agency information systems are developed and maintained.</li><li>• [Agency] shall review plans of action and milestones for consistency with the agency risk management strategy and agency-wide priorities for risk response actions.</li></ul> <p>Information Security Measures of Performance (PM 6)</p> <ul style="list-style-type: none"><li>• [Agency] shall develop, monitor, and report on the results of information security measures of performance.</li></ul>

---

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	<a href="http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx">http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</a>

---

DRAFT

## 1.2 Security Organization (Roles and Responsibilities)

Purpose	The purpose of the Security Organization (Roles and Responsibilities) section is to establish key principles based on which [Agency] Security Organization shall be established.
Policy	<p>Information Security Authority (2.2.3.1)</p> <ul style="list-style-type: none"> <li>[Agency] Director shall ensure that [Agency] senior officials are given the necessary authority to secure the operations and assets under their control.</li> </ul> <p>Senior Information Security Officer (PM 2)</p> <ul style="list-style-type: none"> <li>[Agency] shall appoint a Chief Information Security Officer (CISO) and Chief Information Officer (CIO) with the mission and resources to: coordinate, develop, implement, and maintain an agency-wide information security program.</li> </ul> <p>Information Security Workforce (PM 13)</p> <ul style="list-style-type: none"> <li>[Agency] shall establish an information security workforce and professional development program.</li> </ul> <p>Role-based Security Training (AT 3)</p> <ul style="list-style-type: none"> <li>[Agency] shall provide role-based security training to personnel with assigned security roles and responsibilities.</li> </ul>
Policy Supplement	A policy supplement has not been identified.
Guidance	<p>NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer</p> <p>NIST SP 800-53 Revision 4: PM 13 Information Security Workforce</p> <p>NIST SP 800-53 Revision 4: AT 3 Role-based Security Training</p> <p>NIST SP 800-100: 2.2.3.1 Agency Head</p>
Reference	<p><a href="http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx">http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</a></p> <p><a href="http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf">http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf</a></p>

### 1.3 Information Security Policy Management

---

#### Purpose

The purpose of the Information Security Policy Management section is to establish key principles based on which [Agency] security policies shall be developed. These principles shall function as the foundation on which the security policy statements shall be defined and implemented

---

#### Policy

##### Policy Development

- [Agency] shall adopt a risk-based approach to identify State and agency specific information security objectives for policy gaps, and shall develop information security policies in alignment with the identified security objectives.
  - [Agency] shall allocate the appropriate subject matter experts to the development of State and agency specific information security policies.
  - [Agency] shall approach independent external (third party) specialist to assist in the development of information security policies in cases where it is established that the required skills do not exist within [Agency] or any other agencies within the state.
  - [Agency] shall work in collaboration with other states, Federal government and external special interest groups in cases where policies directly or indirectly affect interfacing activities with other states or the Federal government.
  - Information security policies that are developed at [Agency] shall, at a minimum, contain the following information:
    - 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 [Agency] security policies, 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
    - Exception shall be consistently evaluated in accordance with [Agency] risk acceptance practice.
  - [Agency] shall review the draft policy with stakeholders that shall be impacted by the policy to ensure that the policy is enforceable
-

---

and effective.

- [Agency] shall identify gaps within the policy that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.
- [Agency] shall develop and implement a communication plan to disseminate new policies or changes to existing policies.
- [Agency] shall reviewed policies on an annual basis to ensure that policies are up-to-date and aligned with the State's risk posture.

#### Policy Review and Approval

- A policy governance committee shall be established for the purpose of policy review and approval of policies.
- Policy exemptions shall be explicitly approved by the policy approval governing committee.
- Policy approval history shall be documented in detail.

#### Policy Implementation

- [Agency] shall implement mechanisms to help ensure that information security policies will be available to [Agency] personnel on a continuous basis and whenever required.
- [Agency] shall require employees to review and acknowledge understanding of information security policies 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	<a href="http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx">http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</a>

---

## DEFINITIONS

---

**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.

**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 [Agency] 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.

**Senior information security officer:** Official responsible for carrying out the Chief Information Officer responsibilities under the Federal Information Security Management Act (FISMA) and serving as the Chief Information Officer's primary liaison to the agency's authorizing officials, information system owners, and information system security officers.

**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.