DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – IT Risk Strategy

V0.1 – April 21, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
3/07/2014	Division of Information Security	IT Risk Strategy	1.0	Initial draft
4/21/2014	Division of Information Security	IT Risk Strategy	1.0	Final version – No changes from initial draft

Table of Contents

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.

This policy, along with other information security policies released by the Division of Information Security (DIS), provides 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 statewide information security policies, procedures, and recommended technology solutions
- Providing technical assistance, advice, and recommendations concerning information security matters

(B) Agency/Institution

Information security is a 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, including but not limited to updating agency/institution local policies, standards, and procedures to adopt
- Implementing and maintaining an Information Security Program
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency information security program
- Ensuring that security is part of the information planning and procurement process
- Participating in annual information systems data security self-assessments focusing on compliance to this State information security policies
- 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
- Implement security policies and procedures to help ensure 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 will 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 relation 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

IT Risk Strategy

1.1 Security Performance and Metrics

Purpose	The purpose of the Security Performance and Metrics section is to establish controls to assess the performance of the security program and its components.
Policy	Information Security Measures of Performance (PM 6) • [Agency] shall develop, monitor, and report on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program. • [Agency]-defined performance measures should be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement. Manageability of Metrics (3.4.2) • [Agency] shall ensure that the metrics/ measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps. Data Management Concerns (3.4.3) • [Agency] shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PM 6 Information Security Measures of Performance NIST SP 800-55 Revision 1: 3.4.2 Manageability NIST SP 800-55 Revision 1: 3.4.3 Data Management Concerns
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Third Party Risk Management

Purpose

The purpose of the Third Party Risk Management section is to establish the controls to safeguard [Agency] information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.

Policy

External Information System Services (SA 9)

- [Agency] shall establish a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.
- [Agency] shall implement processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis.

Risk Assessment (RA 3)

- [Agency] shall establish a process to conduct risk assessments on third party service providers, and document the risk assessment results.
- [Agency] shall implement controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties.

System Interconnections (CA 3)

- [Agency] shall authorize connections from [Agency] information systems to third party information systems by entering into Interconnection Security Agreements.
- For each third party interface, [Agency] shall document the interface characteristics, security requirements, and the nature of the information communicated.

Use of External Information Systems (AC 20)

- [Agency] shall establish terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.
- Terms and conditions established by [Agency] should control:
    - Access to [Agency] information systems from third party information systems; and
    - Controls for processing, storing, or transmit of [Agency] data using third party information systems.
- [Agency] shall review and update third party security agreements on an annual basis, or as defined in the contract.

Information Sharing with Third Parties (UL 2)

- [Agency] shall share personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.

	• [Agency] shall, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used. • [Agency] shall monitor, audit, and train its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data. • [Agency] shall evaluate any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems NIST SP 800-53 Revision 4: CA 3 System Interconnections NIST SP 800-53 Revision 4: PS 6 Access Agreements NIST SP 800-53 Revision 4: RA 3 Risk Assessment NIST SP 800-53 Revision 4: SA 9 External Information System Services NIST SP 800-53 Revision 4: UL 2 Information Sharing with Third Parties
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization (to operate): The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other agencies, and the State based on the implementation of an agreed-upon set of security controls.

Developer: A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

Enterprise Architecture: A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Information owner: The person who has been identified as having the ownership of the information asset.

Information resources (IR): Any and all computer printouts, online display devices, magnetic storage media, and all computer-related activities involving any device capable of receiving email, browsing Web sites, or otherwise capable of receiving, storing, managing, or transmitting electronic data including, but not limited to, mainframes, servers, personal computers, notebook computers, hand-held computers, personal digital assistants (PDA), pagers, distributed processing systems, network attached and computer controlled medical and laboratory equipment (i.e. embedded technology), telecommunication resources, network environments, telephones, fax machines, printers and service bureaus. Additionally, it is the procedures, equipment, facilities, software, and data that are designed, built, operated, and maintained to create, collect, record, process, store, retrieve, display, and transmit information.

Information resources manager (IRM): Responsible to the State of South Carolina for management of the [Agency]'s information resources. The designation of an [Agency] information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the [Agency]'s information activities, and ensure greater visibility of such activities within and between state agencies. The IRM has been given the authority and the accountability by the State of South Carolina to implement security policies, procedures, practice standards, and guidelines to protect the information resources of the [Agency]. If the [Agency] does not designate an IRM, the title defaults to the [Agency]'s Executive Director, and the Executive Director is responsible for adhering to the duties and requirements of an IRM.

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

Personally Identifiable Information: Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other agencies, and the State.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Control: A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Sensitive Data: Refers to information protected by State and/or federal law as well as data protected by Agency policies. Following are some prominent examples of sensitive data. Often, context plays a role in data sensitivity; thus, this list is not exhaustive: Social Security number (SSN), credit card number or banking information, passport number, tax information, and credit reports, among others.

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.

Trustworthiness (Information System): The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.