DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Risk Management

v1.0 – October 15, 2013

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/15/2013	Division of Information Security		1.0	Initial draft
2/10/2014	Division of Information Security		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.

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 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 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.
- **Solution Reference:** Provides a reference to the Recommended Technology Solutions in the form of a uniform resource locator (URL).
- **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

Risk Management

1.1 Risk Management

Purpose	The purpose of the risk management section is to define the controls that shall be implemented by [Agency] to identify and assess information security risks, and to take steps to reduce risk to an acceptable level. 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.
Policy	Risk Management Strategy (PM 9) • [Agency] shall define a schedule for an on-going risk assessment and risk mitigation process. • [Agency] shall review and evaluate risk based on the system categorization level and/or data classification of their systems.
Policy Supplement	A risk self-assessment tool has been created by the Division of Information Security. This tool can be leveraged by Agencies/Institutions to perform a risk assessment based on a risk framework developed for the State. See self-assessment tool at https://www.bcbis.sc.gov/DIS/DIS-index.phtm
Solution Reference	An enterprise solution has currently not been identified for this section.
Guidance	NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Risk Assessment

Purpose	The purpose of the risk assessment section is to define a process to identify and manage IT security risks and ensure ongoing compliance with applicable State laws and regulations.
Policy	Risk Assessment (RA 3) • The [Agency] shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards (e.g., NIST 800-30). This assessment framework shall clearly define accountability, roles and responsibilities. Security Assessment (CA 2) • [Agency] 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 (e.g., NIST SP 800-115). • [Agency] shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the [Agency]. Plan of Action and Milestones (CA 5) • [Agency] shall develop and periodically update a Plan of Action & 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. • [Agency] 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 [Agency] systems. Security Authorization (CA 6) • [Agency] 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 [Agency] shall make a decision regarding risk treatment. Continuous Monitoring (CA 7) • [Agency] shall continuously monitor the security controls within its information systems to ensure that the controls are operating as intended.
Policy Supplement	A policy supplement has not been identified.
Solution Reference	An enterprise solution has currently not been identified for this section.
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
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Risk Mitigation

Purpose	The purpose of the risk mitigation section is to support mitigation of risks identified and to define the level of risk that is acceptance to the [Agency] where risks are accepted knowingly and objectively.
Policy	Continuous Monitoring (CA 7) • [Agency] 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. • [Agency] 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].
Policy Supplement	A policy supplement has not been identified.
Solution Reference	An enterprise solution has currently not been identified for this section.
Guidance	NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Authentication: The process of establishing confidence in user identities through a well specified message exchange process that verifies possession of valid credential.

Authorization: Authorization is the process of enforcing policies, and determining what types or qualities of activities, resources, or services a user is permitted. Authorization occurs within the context of authentication. Once a user has been authenticated, they may be authorized for different types of access.

Brute force attacks: A method of accessing an obstructed device through attempting multiple combinations of alphanumeric passwords.

Cryptography: A method of converting clear text into undecipherable text and later reversing the process to create readable text.

Data at rest: All data in storage, regardless of the storage device. This excludes information traversing a network or temporarily residing in non-volatile computer memory. Data at rest primarily resides in files on a file system. However, data at rest is not limited to file data. Databases, for example, are often backed by data files, and their contents can be thought of as rows and columns of data elements instead of as individual files. Agency should consider all aspects of storage when designing an encryption solution.

Degaussing: Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.

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, tablets, mobile computers, 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.

Least privilege: Every program and every user of the system should operate using the least set of privileges necessary to complete the job. Primarily this principle limits the damage that can result from an accident or error. - This principle requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks only for the minimum amount of time necessary. The application of this principle limits the damage that can result from accident, error, or unauthorized use or activity.

Media sanitization: Media sanitization is a process by which data is irreversibly removed from media or the media is permanently destroyed. There are different types of sanitization for each type of media including: disposal, clearing, purging and destroying.

Obfuscation: Data masking or data obfuscation is the process of de-identifying (masking) specific data elements within data stores. The main reason for applying masking to a data field is to protect data that is classified as personal identifiable data, personal sensitive data or commercially sensitive data; however the data must remain usable for the purposes of undertaking valid test cycles.

Privacy Officer: The Privacy Officer shall oversee all ongoing activities related to development, implementation and maintenance of the Agency's privacy policies in accordance with applicable federal and State laws.

RBAC: A role based access control (RBAC) policy bases access control decisions on the functions a user is allowed to perform within an Agency. The users cannot pass access permissions on to other users at their discretion. A role is essentially a collection of permissions, and all users receive permissions only through the roles to which they are assigned, or through roles they inherit through the role hierarchy. Within an Agency, roles are relatively stable, while users and permissions are both numerous and may change rapidly.

Segregation of Duties: The separation of duties to prevent conflicts of interest and ensure that no changes are executed without being observed by another individual. The purpose of the control is to minimize fraud, error, and omission.

System development life cycle (SDLC): A multistep process to develop or acquire systems that starts with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

Two-factor authentication (2FA): Authentication systems identify three factors as the cornerstone of authentication: something you know (for example, a password); something you have (for example, an ID badge or a cryptographic key); something you are. Two-factor authentication refers to the use of two of these three factors listed above.