# DIVISION OF INFORMATION SECURITY (DIS)

# Information Security Policy – IT Compliance

V1.0 – March 7, 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 Compliance | 1.0 | Initial draft |
| | | | | |
| | | | | |
| | | | | |
| | | | | |

# Table of Contents

## 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.
- **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 Compliance

### 1.1 Audit and Compliance Requirements

| | |
|---|---|
| Purpose | The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance of with information security policies and standards at State agencies and institutions. |
| Policy | Compliance with legal and contractual requirements (A.15.1)<br>• [Agency] shall identify and document its obligations to applicable State, federal and other third party laws and regulations in relation to information security.<br>Compliance with security policies and standards (A.15.2.1, A.15.2.2)<br>• At least annually, [Agency] shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary.<br>• Results from compliance reviews or audits shall be documented, and reported to [Agency] leadership.<br>Audit and Accountability Policy and Procedures (AU 1)<br>• [Agency] shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures.<br>• [Agency] shall implement a process to review and update the audit and accountability policy and associated procedures at least annually. |
| Policy Supplement | A policy supplement has not been identified. |
| Guidance | ISO 27001:2005: A.15.1 Compliance with legal and contractual requirements<br>ISO 27001:2005: A.15.2.1 Compliance with security policies and standards<br>ISO 27001:2005: A.15.2.2 Technical compliance checking<br>NIST SP 800-53 Revision 4: AU 1 Audit and Accountability Policy and Procedures |
| Reference | http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx |

## 1.2 Information System Audit Considerations

| | |
|---|---|
| Purpose | The purpose of the IS Audit Considerations section is to establish controls and processes to maximize the effectiveness of and to minimize interference to/from the information systems audit process. |
| Policy | Information systems audit controls (A.15.3.1)<br>• [Agency] shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.<br>Protection of information systems audit tools (A.15.3.2)<br>• [Agency] shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.<br>Audit Events (AU 2)<br>• [Agency] shall determine the type of events that are to be audited within information systems.<br>• [Agency] shall review and update the list of audited events annually.<br>• [Agency] leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.<br>Content of Audit Records (AU 3)<br>• [Agency] information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.<br>Audit Records Review and Reporting (AU 6)<br>• [Agency] shall analyze information system audit records periodically.<br>• [Agency] shall report findings of audit records reviews to information security personnel and [Agency] leadership.<br>• [Agency] shall perform correlation and analysis of information generated by security assessments and monitoring.<br>Audit Storage Capacity (AU 4)<br>• [Agency] shall allocate sufficient audit storage capacity to help ensure compliance with audit logs retention requirements from State, federal, and other applicable third party laws and regulations.<br>• [Agency] shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited. |
| Policy Supplement | A policy supplement has not been identified. |

| | |
|---|---|
| Guidance | ISO 27001:2005: A.15.3.1 Information systems audit controls<br>ISO 27001:2005: A.15.3.2 Protection of information systems audit tools<br>NIST SP 800-53 Revision 4: AU 2 Audit Events<br>NIST SP 800-53 Revision 4: AU 3 Content of Audit Records<br>NIST SP 800-53 Revision 4: AU 4 Audit Storage Capacity<br>NIST SP 800-53 Revision 4: AU 6 Audit Review, Analysis, and Reporting |
| Reference | http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx |

## 1.3 Information Security Continuous Monitoring

| | |
|---|---|
| Purpose | The purpose of the Information Security Continuous Monitoring policy is to establish controls that will provide State agencies and institutions the effective monitoring and response capabilities in relation to compliance issues and incidents. |
| Policy | Continuous Monitoring (CA 2)<br>• [Agency] shall employ assessment teams to monitor the security controls on an ongoing basis.<br>• [Agency] assessment teams shall be independent from operational or business functions, or hired third parties.<br>Plan of Action and Milestones (CA 5)<br>• [Agency] shall develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as result of internal/external risk assessments, security reviews, and/or audits.<br>• [Agency] shall update its plan of action and milestones at least on a yearly basis, and also based on the findings from continuous security monitoring activities. |
| Policy Supplement | A policy supplement has not been identified. |
| Guidance | NIST SP 800-53 Revision 4: CA 2 Security Assessments<br>NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones |
| Reference | http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx |

## DEFINITIONS

**Auditable event:** A system activity identified by the entity's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.

**Authentication:** The process of establishing confidence in user identities through a well specified message exchange process that verifies possession of a password, token to remotely authenticate a claimant.

**Authorization:** Authorization is the process of enforcing policies: 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.

**Chief Information Officer**: The agency official responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, information policies and information resources management responsibilities, including information security and the management of information technology.

**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.

**Information System**: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

**Information System Owner**: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.