# DIVISION OF INFORMATION SECURITY (DIS)

# Information Security Policy – Information Systems Acquisitions, Development, and Maintenance

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 are associated 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 uniform resource locator (URL) reference to the Recommended Technology Solutions.
- **Guidance:** Provides references to guidelines on information security policies.
- **Reference:** Provides a uniform resource locator (URL) reference to the guidance.

# INFORMATION SECURITY POLICY

# Information Systems Acquisitions, Development, and Maintenance

## 1.1 Change Management

Purpose

The purpose of the change management section is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner to production, and applicable non-production environments with minimal impact and risk.

- Policy

Configuration Change Control (CM 3)

- [Agency] shall define change management controls to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors. The implementation of changes shall be controlled through the use of a change control process. The following recommendations shall be followed for the change control process:
    - All requests for change shall be handled in a structured way that determines the impact on the operational system and its functionality;
    - All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner.
    - [Agency] shall have a process to categorize, prioritize and authorize changes to information systems;
    - Post-implementation reviews shall be performed to ensure production changes are operating as intended;
    - A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;
    - A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; and
    - Information systems shall be reviewed and tested after major changes to operating systems.

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: CM 3 Configuration Change Control

Reference

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

## 1.2 Configuration Management

**Purpose**

The purpose of the configuration management section is to establish procedures for the compliance with minimally acceptable system configuration requirements, as determined by [Agency]. In addition, this section helps ensure [Agency] establish processes to identify and implement secure configurations, control configuration changes, and monitor security controls to validate adherence with approved configurations.

**Policy**

Baseline Configuration (CM 2)

- [Agency] shall develop, review, and formally approve baseline configurations (most secure state) for critical information systems and infrastructure components.
- [Agency] shall develop a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.
- [Agency] shall establish a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.
- [Agency] shall retain older versions of baseline configurations to be able to support rollback.
- [Agency] shall review and update baseline configurations periodically, and/or as an integral part of information system component installations or upgrades.

Configuration Management Plan (CM 9)

- The [Agency] shall assign responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.

**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: CM 2 Baseline Configuration
NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan
NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems

**Reference**

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

## 1.3 System Development and Maintenance

Purpose

The purpose of the system development and maintenance section is to define requirements for system security planning and to improve protection of [Agency] information system resources.

Policy

System Security Plan (PL 2)

- [Agency] shall prepare system security plans and documentation for critical enterprise information systems or systems under development.
- System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.
- When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

Vulnerability Scanning (RA 5)

- [Agency] shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.
- [Agency] shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.
- Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.

System and Services Acquisition Policy and Procedures (SA 2)

- [Agency] shall develop and follow a set of procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.
- [Agency] shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

System Development Life Cycle (SA 3)

- [Agency] shall implement appropriate security controls at all stages of the information system life cycle

External Information System Services (SA 9)

- [Agency] shall supervise and monitor outsourced software development to validate [Agency] security requirements.

Developer Security Testing and Evaluation (SA-11)

- [Agency] shall establish separate development, testing, and production environments
- [Agency] shall not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval,

procedures to remove/delete data after completion of tests, and documentation of activities, shall be implemented.

Flaw Remediation (SI 2)

- [Agency] shall design appropriate controls into information systems, including user developed applications to ensure correct processing.
- [Agency] shall ensure that software patches are applied when they function to remove or reduce security weaknesses.

Security Alerts, Advisories, and Directives (SI 5)

- [Agency] shall establish a process to collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.
- A specific group or individual shall be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

Software, Firmware, and Information Integrity (SI 7)

- [Agency] shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).
- [Agency] shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

Information Input Validation (SI 10)

- [Agency] shall incorporate controls into information systems to check the validity of information inputs and information outputs.
- [Agency] shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

Session Authenticity (SC 23)

- [Agency] shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

| | |
|---|---|
| Policy Supplement | Threat and Vulnerability Management 1.1: Patch Management<br>Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution |
| Solution Reference | Refer to the *Division of Information Security* website for available enterprise solutions. |

Guidance

NIST SP 800-53 Revision 4: PL 2 System Security Plan
NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning
NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure
NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle
NIST SP 800-53 Revision 4: SA 9 External Information System Services
NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation
NIST SP 800-53 Revision 4: SI 2 Flaw Remediation
NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity
NIST SP 800-53 Revision 4: SI 10 Information Input Validation
NIST SP 800-53 Revision 4: SC 23 Session Authenticity

Reference

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

## 1.4 Release Management

Purpose

The purpose of the release management section is to define the appropriate release activities during an implementation or upgrade of information systems.

Policy

Allocation of Resources (SA 2)

- [Agency] shall ensure that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build and test, pilot, and deploy).
- [Agency] shall determine as part of the release planning process:
    - Resources required to deploy the release;
    - Pass/fail criteria;
    - Build and test plans prior to implementation;
    - Pilot and deployment plans; and
    - Develop requirements for the release.

Information System Documentation (SA 5)

- [Agency] shall document the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release;
- [Agency] shall validate the release design against the requirements, and identify the risks and potential issues.

Security Engineering Principles (SA 8)

- [Agency] shall implement standardization and enforce operational controls through the use of change requests for deploying releases into production.

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: SA 2 Allocation of Resources<br>NIST SP 800-53 Revision 4: SA 5 Information System Documentation<br>NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles |
| 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.