**<INSERT AGENCY LOGO>**

**<INSERT AGENCY NAME>**

**Information Security Plan (ISP)**

|  |
| --- |
| Month Day, Year |
|  |
| **This document contains confidential information for <AGENCY> Official Use Only. It shall not be duplicated, used, or disclosed in whole or in part without prior written permission from the Information Security Staff.** |

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version Number** | **Date** | **Author(s)** | **Description** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Table of Contents

About This Document 4

Who should use this document? 4

Executive Summary 4

AGENCY IDENTIFICATION 5

PERSONNEL CONTACTS 5

APPLICABLE LAWS OR REGULATIONS 7

OPEN/CLOSED ASSESSMENTS ITEMS (Audit reports, Gap Analysis, etc.) 7

SECURITY CONTROLS DETAILS AND COMMENTS 8

Asset Management 8

Access Control 8

Business Continuity Management 8

Data Protection and Privacy 8

Human Resources (HR) and Security Awareness 8

IT Compliance 9

IT Risk Strategy 9

Information Systems Acquisitions, Development, and Maintenance 9

Mobile Security 10

Physical Environmental Security 10

Risk Management 10

Threat Vulnerability Management 11

APPENDICIES AND ATTACHMENTS 12

Attachment A - <TITLE> 12

DEFINITIONS 13

REFERENCES 13

# About This Document

This document is provided in template format. Once populated with details, this document will deliver details covering information about <AGENCYNAME>’s information security controls. The use of this template is not required. It serves as a minimum representation of the information required.

The Information Security Plan is the main document in which the agency documents all the security related information. The security plan for the agency-wide information security program provides complete coverage for all security controls employed within the agency.

# Who should use this document?

This document provides South Carolina State agencies a template to be used by <AGENCYNAME>’s. It supports an agencies responsibility for implementing the South Carolina INFOSEC program, as detailed by the Division of Information Security.

This template also provides a document with organizational information security controls for the purpose of managing an information security infrastructure. Systems are difficult to manage without a documented understanding of how the infrastructure is architected.

# Executive Summary

State of South Carolina agencies are required to identify each information system that contains, processes, and transmits state data and information and implement the plan for the security and privacy provided by the State of South Carolina. The objective of the security plan is to improve protection of information technology (IT) resources. All State of South Carolina systems require protection as part of the FY14-15 Provisos (117.113 and 101.32). The protection of the agency must be documented in a security plan.

The security plan reflects input from management responsible for the system, including information owners, the system operator, the system security manager, and system administrators.

The purpose of this security plan is to provide an overview of the security of <AGENCYNAME> and describe the controls and critical elements in place or planned. Each applicable security control must be identified as either in place or planned. This ISP follows guidance contained in NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems, February 2006.*

The ISP is a living document that will be updated periodically to incorporate new and/or modified security controls. The plan will be revised as the changes occur to the system, the data or the technical environment in which the system operates.

# AGENCY IDENTIFICATION

|  |  |
| --- | --- |
| **Identifier** | **Response Data** |
| **Agency Name:** |  |
| **Agency Acronym:** |  |
| **Agency Code:** |  |
| **Agency Director:** |  |
| **Agency Director Contact Info:** |  |

## PERSONNEL CONTACTS

System personnel contacts include contact information for the information security authority, information security liaison, and other designated contacts. See definitions for additional contact descriptions.

|  |  |
| --- | --- |
| **Information Security Authority** | **Response Data** |
| **Name:** |  |
| **Title:** |  |
| **Agency:** |  |
| **Division:** |  |
| **Physical Address:** |  |
| **City, State, Zip:** |  |
| **E-Mail:** |  |
| **Primary Phone:** |  |

|  |  |
| --- | --- |
| **Policy Champion** | **Response Data** |
| **Name:** |  |
| **Title:** |  |
| **Agency:** |  |
| **Division:** |  |
| **Physical Address:** |  |
| **City, State, Zip:** |  |
| **E-Mail:** |  |
| **Primary Phone:** |  |

|  |  |
| --- | --- |
| **Information Security Liaison** | **Response Data** |
| **Name:** |  |
| **Title:** |  |
| **Agency:** |  |
| **Division:** |  |
| **Physical Address:** |  |
| **City, State, Zip:** |  |
| **E-Mail:** |  |
| **Primary Phone:** |  |

|  |  |
| --- | --- |
| **Information Security Workforce** | **Response Data** |
| **Name:** |  |
| **Title:** |  |
| **Agency:** |  |
| **Division:** |  |
| **Physical Address:** |  |
| **City, State, Zip:** |  |
| **E-Mail:** |  |
| **Primary Phone:** |  |

|  |  |
| --- | --- |
| **Information Security Workforce** | **Response Data** |
| **Name:** |  |
| **Title:** |  |
| **Agency:** |  |
| **Division:** |  |
| **Physical Address:** |  |
| **City, State, Zip:** |  |
| **E-Mail:** |  |
| **Primary Phone:** |  |

*<Add/Remove INFORMATION SECURITY WORKFORCE tables as needed>*

## APPLICABLE LAWS OR REGULATIONS

The list of the Applicable Laws or Regulations is provided in this section.

## OPEN/CLOSED ASSESSMENTS ITEMS (Audit reports, Gap Analysis, etc.)

In this section include open or closed IT audit findings, risk derived findings, internal assessments, at the time of approval of the security plan.

|  |  |  |  |
| --- | --- | --- | --- |
| *Date the item was opened* | *Finding/Gap summary, including related security controls* | *Assessment type (SOX; HIPAA; IRS; Gap; etc.)*  | *Date closed or to be remediated* |
|  |  |  |  |

# SECURITY CONTROLS DETAILS AND COMMENTS

*Instruction: In the sections that follow, document the location of the agency’s policy, procedure, guidelines, and/or additional supporting documentation****. For all control categories, include the gap analysis and implementation plan****. It is assumed State IFOSEC policies are adopted by all agencies unless otherwise noted in sections below. A list of example documents is provided within each section. The lists serves as examples only, DIS can provide assistance if further explanation is needed.*

## Asset Management

*Examples of items expected:*

* *Procedure for identifying assets*
* *Asset inventory and security impact analysis with data classification*

## Access Control

*Examples of items expected:*

* *New Hire data access procedure,*
* *Export of system logon notice,*
* *Network diagrams that detail remote access,*
* *Procedure for remote administration and access,*
* *Export of Active Directory; LDAP; or RACF password settings*

## Business Continuity Management

*Examples of items expected:*

* *Disaster Recovery Plan (DRP)*
* *Business Continuity Plan (BCP)*
* *Business Impact Analysis*
* *BCP and DRP training*
* *Tape backup process*

## Data Protection and Privacy

*Examples of items expected:*

* *Security planning policy and procedures*
* *Security categorization documentation*
* *Procedures addressing media sanitization and disposal*
* *Media sanitization records*
* *Procedures addressing cryptographic key management and establishment*
* *Information system design documentation*
* *Procedures addressing transmission confidentiality*
* *Privacy Impact Assessment*

## Human Resources (HR) and Security Awareness

*Examples of items expected:*

* *Transfer procedures*
* *New hire checklist*
* *Procedures addressing personnel termination*
* *Records of personnel termination actions*
* *Security training curriculum*
* *Training records*
* *Procedures addressing security training implementation*
* *Awareness media*

## IT Compliance

*Examples of items expected:*

* *Procedures addressing security assessments*
* *Information Security Plan*
* *Gap analysis of existing policy and standards against legal/contracts*
* *Audit reports (internal/external)*
* *Information system configuration settings*
* *List of information system auditable events*
* *Information system audit records*
* *Procedures addressing content of audit records*
* *Procedures addressing security assessments*
* *Security assessment plan*
* *Policy plan of action*
* *POA&Ms*

## IT Risk Strategy

*Examples of items expected:*

* *Security measures of performance*
* *Reports with information security measures of performance*
* *Metrics list with defined purpose*
* *Procedures addressing external information system services*
* *Service-level agreements*
* *Risk assessment results*
* *Risk assessment reviews*
* *Information system Interconnection Security Agreements*
* *Information system design documentation*
* *External information systems terms and conditions*
* *List of types of applications accessible from external information systems*
* *MOAs/MOUs*

## Information Systems Acquisitions, Development, and Maintenance

*Examples of items expected:*

* *Systems Interconnection agreements,*
* *SDLC procedure,*
* *Systems hardening standards,*
* *Change management procedures,*
* *Code testing procedure,*
* *Previous vulnerability reports, etc.*

## Mobile Security

*Example of items expected:*

* *System use policy*
* *Procedures addressing media usage restrictions*
* *Procedures addressing access control for mobile device usage (including restrictions)*
* *Authorizations for mobile device connections*
* *Information system audit records*
* *Documentation of encryption mechanisms*
* *Procedures addressing media storage*
* *Logs of media transport*
* *Logs of media destruction*
* *Media inventory*

## Physical Environmental Security

*Example of items expected:*

* Physical security plan
* *Authorized personnel access list*
* *Physical access termination records*
* *List of positions/roles and corresponding physical access authorizations*
* *List of security safeguards controlling access*
* *Information system entry and exit points*
* *Facility layout*
* *Physical access log reviews*
* *Visitor access control logs*
* *Uninterruptible power supply test record*
* *Disaster recovery plan*
* *Test records of fire suppression and detection devices/systems*
* *Logs of media destruction*
* *Media inventory*

## Risk Management

*Examples of items expected:*

* *Risk assessment*
* *Risk assessment results*
* *Procedures addressing security assessments*
* *Security assessment results*
* *Agency risk acceptance forms*
* *POA&Ms*
* *Corrective Action Plans (CAP)*
* *Procedures addressing configuration management*
* *Information system monitoring records*
* *Security impact analyses*
* *Security assessment report*

## Threat Vulnerability Management

*Examples of items expected:*

* *Procedures addressing vulnerability scanning*
* *Security assessment report*
* *Vulnerability scanning results*
* *Patch and vulnerability management records*
* *Penetration test report*
* *Procedures addressing penetration testing*
* *Incident response plan*
* *Procedures addressing incident handling*
* *Information system design documentation*
* *Procedures addressing information system monitoring tools and techniques*
* *Locations within information system where monitoring devices are deployed*
* *Incident response training logs and media*
* *Procedures addressing configuration management*
* *List of flaws and vulnerabilities potentially affecting the information system*
* *Test results from flaw scanning*
* *Installation/change control records for security-relevant software and firmware updates*

# APPENDICIES AND ATTACHMENTS

##

## Attachment A - <TITLE>

If included, the description of the attachment is provided in this section.

# DEFINITIONS

**Agency** – refers to all South Carolina state agencies, institutions, departments, divisions, boards, commissions, and authorities

**CAP**- Corrective Action Plan is used to identify activities planned of completed to correct deficiencies.

**DIS** – Division of Information Security - The Division is responsible for a variety of statewide polices, standards, programs and services relating to cyber security and information systems, including the statewide coordination of critical infrastructure information.

**INFOSEC** – Commonly used abbreviation for Information Security.

**Information Security Authority** – The agency’s chief executive

**Information Security Liaison** - Official responsible for carrying out the “Chief Information Officer” responsibilities within the agency under the Federal Information Security Management Act (FISMA) and serving as the primary liaison between the DIS office of the Chief Information Security Officer and the agency’s authorizing officials, information system owners, and information system security officers.
**Information Security Workforce –** Personnel with Information Security responsibilities.
**LDAP** – Lightweight Directory Access Protocol that allows computing platforms the ability to access directory information.
**POA&M** - Plan of Actions and Milestones describes tasks that are planned to correct any weaknesses or deficiencies with security controls.

* **Policy Champion** - Individual with a management role in the areas of compliance, information security (InfoSec) and/or technology
**RACF** - Resource Access Control Facility provides security policies and permissions to data and objects. It is commonly used as an authentication source for IBM mainframe systems.

# REFERENCES

NIST Special Publication (SP) 800-18 Rev. 1, *Guide for Developing Security Plans for Federal Information Systems, February 2006.*

NIST Special Publication (SP) 800-53a Rev. 1, *Guide for Assessing the Security Controls in Federal Information Systems and Organizations, June 2010.*

Cloud CIO, *FedRAMP System Security Plan Template v2.0, June 2014.*

Centers for Medicare & Medicaid Services, *CMS\_SSP\_Template\_v3.1*, May 2009.

GTA-Office of Information Security, *Information System Security Plan Template*, 2012