# DIVISION OF INFORMATION SECURITY (DIS)

# Information Security Policy – Physical & Environmental Security

V1.0 – 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 | Physical & Environmental Security | 1.0 | Initial draft |
| 4/21/2014 | Division of Information Security | Physical & Environmental 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.
- **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

## Physical & Environmental Security

### 1.1 Physical Access and Security

| | |
|---|---|
| Purpose | The purpose of the Physical Access and Security section is to establish controls to prevent unauthorized physical access to [Agency] information assets to protect them from damage, interruption, misuse, destruction and/ or theft. |
| Policy | Physical and Environmental Protection Policy and Procedures (PE 1)<br>• [Agency] shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.<br>• [Agency] shall establish procedures to review and maintain current the physical and environmental protection policy and associated procedures.<br>Physical Access Authorizations (PE 2)<br>• [Agency] shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.<br>• [Agency] shall establish a process to review, approve, and issue credentials for facility access.<br>• [Agency] shall remove individuals from the facility access list when access is no longer required.<br>Physical Access Control (PE 3)<br>• [Agency] control entry to / exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).<br>• [Agency] shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.<br>• [Agency] shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.<br>• [Agency] shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.<br>• [Agency] shall establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.<br>• [Agency] shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated. |

| | |
|---|---|
| | Access Control for Transmission Medium (PE 4)<br>• [Agency] shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).<br>Access Control for Output Devices (PE 5)<br>• [Agency] shall place output devices in secured areas and in locations that can be monitored by authorized personnel, and allow access to authorized individuals only.<br>• [Agency] shall control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.<br>Monitoring Physical Access (PE 6)<br>• [Agency] shall review physical access logs at a defined frequency and upon occurrence of security incidents.<br>Visitor Access Records (PE 8)<br>• [Agency] shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of 1 year.<br>Delivery and Removal (PE 16)<br>• [Agency] shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items. |
| Policy Supplement | A policy supplement has not been identified. |
| Guidance | NIST SP 800-53 Revision 4: PE 1 Physical and Environmental Protection Policy and Procedures<br>NIST SP 800-53 Revision 4: PE 2 Physical Access Authorizations<br>NIST SP 800-53 Revision 4: PE 3 Physical Access Control<br>NIST SP 800-53 Revision 4: PE 4 Access Control for Transmission Medium<br>NIST SP 800-53 Revision 4: PE 5 Access Control for Output Devices<br>NIST SP 800-53 Revision 4: PE 6 Monitoring Physical Access<br>NIST SP 800-53 Revision 4: PE 8 Visitor Access Records<br>NIST SP 800-53 Revision 4: PE 16 Delivery and Removal |
| Reference | N/A |

## 1.2 Environmental Security

| | |
|---|---|
| Purpose | The purpose of the Environmental Security section is to define controls to protect [Agency] information assets from damage, destruction and/ or interruption due to environmental factors such as fire, humidity, water, power outage, etc. |
| Policy | Power Equipment and Cabling (PE 9)<br>• [Agency] shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.<br>Emergency Shutoff (PE 10)<br>• [Agency] shall make available the capability of shutting off power to data center(s) during an incident.<br>• [Agency] shall place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.<br>• [Agency] shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.<br>Data Center Emergency Power (PE 11)<br>• [Agency] shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.<br>Data Center Fire Protection (PE 13)<br>• [Agency] shall install and maintain fire detection and suppression devices that are supported by an independent power source.<br>• [Agency] shall employ fire detection devices/ system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.<br>• [Agency] shall employ an automatic fire suppression system if/ when the data center(s) is not staffed on a continuous basis.<br>Data Center Temperature and Humidity Controls (PE 14)<br>• [Agency] shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.<br>• [Agency] shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.<br>Data Center Water Damage Protection (PE 15)<br>• [Agency] shall protect processing equipment from damage resulting from water leakage. |
| Policy Supplement | A policy supplement has not been identified. |
| Guidance | NIST SP 800-53 Revision 4: PE 9 Power Equipment and Cabling<br>NIST SP 800-53 Revision 4: PE 10 Emergency Shutoff<br>NIST SP 800-53 Revision 4: PE 11 Emergency Power |

| | |
|---|---|
| | NIST SP 800-53 Revision 4: PE 13 Fire Protection<br>NIST SP 800-53 Revision 4: PE 14 Temperature and Humidity Controls<br>NIST SP 800-53 Revision 4: PE 15 Water Damage Protection |
| Reference | N/A |

## 1.3 Disposal of Equipment

| | |
|---|---|
| Purpose | The purpose of the Disposal of Equipment section is to define the controls that shall be followed for disposal of information system equipment which contains [Agency] information. |
| Policy | Media Sanitization (MP 6)<br>• [Agency] shall define and implement mechanisms for disposal of digital media and data storage devices.<br>• [Agency] shall employ sanitization mechanisms with the strength and integrity commensurate with classification of data to be sanitized.<br>• [Agency] shall establish processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.<br>• [Agency] shall implement controls to track and verify sanitization of devices prior to disposal. |
| Policy Supplement | A policy supplement has not been identified. |
| Guidance | NIST SP 800-53 Revision 4: MP 6 Media Sanitization |
| Reference | N/A |

## DEFINITIONS

**Audit Log**: A chronological record of information system activities, including records of system accesses and operations performed in a given period.

**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.

**Availability**: Ensuring timely and reliable access to and use of information.

**Confidentiality**: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

**Degaussing:** Exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.

**Event**: Any observable occurrence in an information system.

**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 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.

**Integrity**: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

**Media:** Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

**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.

**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.

**Sensitive facilities:** Refers to facilities use to store of process sensitive data in physical format (e.g., hard copy documents, tapes, computer equipment containing data) or digital media (e.g., warehouse with computer equipment, hard drives).

**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.

**Threat**: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

**Vulnerability**: Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.