DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Data Protection and Privacy

v1.0 – October 30, 2013

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/30/2013	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 are expected to comply with the State's information security policies and may leverage them in revising existing or developing new 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

Data Protection and Privacy

1.1 Data Classification

Purpose	The purpose of the data classification section is to define the different categories for [Agency] information assets regardless of form whether it is electronic, hard copy, or intellectual property.
Policy	Security Categorization (RA 2)

- [Agency] shall categorize data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. [Agency] data shall be classified into one of the following categories:

  1. **Public:** Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.
  2. **Internal Use:** Information that is used in daily operations of the [Agency]. Examples of internal use information include [Agency] hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the State.
  3. **Confidential**: Confidential information refers to sensitive information in custody of the [Agency]. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.
  4. **Restricted**: Restricted information is highly sensitive information in custody or owned by the [Agency] and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of Restricted data shall result in considerable risk to the State including statutory penalties.

	• Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or the [Agency] Information Security and/or Data Privacy team(s) to determine the appropriate data classification. • If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.
Policy Supplement	Refer to the *Division of Information Security* website for available enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: RA 2 Security Categorization
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Data Disposal

Purpose	The purpose of the data disposal section is to define the controls that shall be followed for disposal of data both in digital and non-digital formats.
Policy	Media Sanitization (MP 6) • [Agency] shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse and release outside of the [Agency] based on applicable regulatory requirements. • [Agency] shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information. • [Agency] shall establish controls mechanism and processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices. • [Agency] shall implement controls to track media sanitization and disposal process, wherein such actions shall be tracked, documented, and verified. • Media sanitization documentation shall provide a record of the media sanitized, when, how media was sanitized, the person who performed the sanitization, and the final disposition of the media. The record of action taken shall be maintained in a written or electronic format. • [Agency] shall test media sanitization equipment and procedures at least annually to ensure correct performance. • FTI Receiving Agency only: [Agency] sanitizing electronic media containing Federal Tax Information shall not make it available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing. • [Agency] shall define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be redeployed outside of the [Agency]. • Approved processes like physical destruction or digital degaussing shall be performed on devices, before they are disposed. • [Agency] shall destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal. • The [Agency] information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: MP 6 Media Sanitization
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Data Protection

Purpose	The purpose of the encryption section is to define the controls that need to be in-place to protect confidential and restricted data.
Policy	System and Communications Protection Policy and Procedures (SC 1) • [Agency] employees shall follow [Agency]'s acceptable use policies when transmitting data. Cryptographic Key Establishment and Management (SC 12) • [Agency] implemented mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users. • [Agency] shall implement mechanisms to ensure the confidentiality of private keys. • [Agency] shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization. • [Agency] shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service. Cryptographic Protection (SC 17) • For Restricted or data protected by Federal or State laws or regulations: [Agency] shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data. • [Agency] shall implement all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption. • [Agency] shall not use any proprietary encryption algorithms for any purpose, unless approved by [Agency]'s information security department. Transmission Confidentiality and Integrity (SC 8 and SC 9) • Confidential or restricted information transmitted as an email message shall be encrypted based on [Agency] encryption policy. • Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with [Agency] shall be encrypted or be transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN), point-to-point tunnel protocols (PPTP) like secure socket layers (SSL). • [Agency] shall implement wireless encryption standards such as Wi-Fi Protected Access 2 (WPA2), and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions that are used for transmitting confidential or restricted

	information. • [Agency] shall utilize encrypted file transfer programs such as "secured File Transfer Protocol (SFTP)" (FTP over Secure Shell (SSH) and Secure Copy (SCP) to secure transfer of documents and data over the Internet. Only authorized users shall be able to initiate secure transactions.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures NIST SP 800-53 Revision 4: SC 8 Transmission Integrity NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management NIST SP 800-53 Revision 4: SC17 Cryptographic Protection
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Privacy

Purpose	The purpose of the privacy section is to set forth policies [Agency] shall use when information systems or applications will gather Personal Identifiable Information (PII) and/or when webpages are available openly to the public.
Policy	Privacy Impact Assessment • [Agency] shall conduct a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII). • [Agency] shall publish privacy policies on [Agency] websites used by the public. • [Agency] shall update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form). • PIAs shall include: a. What information is to be collected (e.g., nature and source); b. Why information is being collected (e.g., to determine eligibility) c. Intended use of information (e.g., to verify existing data); d. With whom the information will be shared; e. What opportunities individuals have to decline to provide information; f. How the information will be secured; • The PIA document shall be reviewed by an [Agency] executive or designee, such as CIO, CISO, or similar. • Each [Agency] is to provide a confidentiality agreement defining the responsibilities of the [Agency]'s employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information. • The [Agency] electronic information privacy officer, in conjunction with the [Agency] human resources department, is responsible for the development and administration of this confidentiality agreement.
Policy Supplement	A policy supplement has not been identified.
Guidance	Fair Information Practice Principles (FIPPs) OMB Memorandum 03-22
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 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.

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

Data at rest: All data in storage, regardless of the storage device, that is not in motion. 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: 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, 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 organization'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 organization. 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 organization, roles are relatively stable, while users and permissions are both numerous and may change rapidly.

SDLC: The multistep process that starts with the initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system, is called the System Development Life Cycle (SDLC).

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. Multi-factor authentication refers to the use of two of these three factors listed above.