DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Human Resource (HR) and Security Awareness

v1.0 – September 25, 2013

Revision History

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

Date	Authored by	Title	Ver.	Notes
9/25/2013	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 standards
- 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 information 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. Overview

Each information security policy 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 requirements and recommendations that are connected to the South Carolina Information Security Standards.
- **Guidance:** Provides references to guidelines on information security policies.

INFORMATION SECURITY POLICY

Human Resource (HR) and Security Awareness

1.1 Human Resource Compliance

Purpose	The purpose of human resource (HR) compliance is to define security roles and responsibilities for employees, contractors and third party users.
Policy	Personnel Security Policy and Procedures (PE 1) • [Agency] shall define security roles and responsibilities of employees, contractors and third party users and shall be documented in accordance with the organization's information security policy. Personnel Screening (PS 3) and Third-Party Personnel Security (PS 7) • [Agency] shall conduct background verification checks on all candidates for employment, including contractors, and third party users, and shall be carried out in accordance with relevant laws. Personnel Termination (PS 4) and Transfer (PS 5) • Upon termination / transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel shall return to the [Agency] all agency documents (and all copies thereof) and other agency property and materials in their possession or control. Access Agreements (PS 6) • As part of their information security obligation, employees, contractors and third party users shall agree and sign an acceptable use policy, which shall state responsibilities for information security.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PE 1 Personnel Security Policy and Procedures NIST SP 800-53 Revision 4: PS 3 Personnel Screening NIST SP 800-53 Revision 4: PS 4 Personnel Termination NIST SP 800-53 Revision 4: PS 5 Personnel Transfer NIST SP 800-53 Revision 4: PS 6 Access Agreements NIST SP 800-53 Revision 4: PS 7 Third-Party Personnel Security

1.2 Security Awareness Training

Purpose	The purpose of security and awareness training is to define the information security training requirements for [Agency] employees, contractors and third party users.
Policy	Security Awareness Training (AT 2) and Information Security Workforce (PM 13) • [Agency] management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. Role-Based Security Training (AT 3) • [Agency] shall impart appropriate awareness training and regular updates in organizational policies and procedures to all employees of the organization and to, contractors and third party users, as relevant for their job function. ○ Training must be accompanied by an assessment procedure based on the cyber security training content presented in order to determine comprehension of key cyber security concepts and procedures. • User access to [Agency] information assets and systems will only be authorized for those users whose cyber security awareness training is current (e.g., having passed the most recent required training stage). Testing, Training, and Monitoring (PM 14) • [Agency] will appoint a cyber-security awareness training coordinator to manage training content, schedules and user training completion status. • The [Agency] cyber security training coordinator, along with the agency CISO or security manager will review training content on an annual basis to ensure that it aligns with State of South Carolina policies.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: AT 2 Security Awareness Training NIST SP 800-53 Revision 4: AT 3 Role-Based Security Training NIST SP 800-53 Revision 4: PM 13 Information Security Workforce NIST SP 800-53 Revision 4: PM 14 Testing, Training, and Monitoring

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: Degaussing is exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic domains.

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.

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.