DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Access Control

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 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

Access Control

1.1 Access Management

Purpose	The purpose of the access management section is to establish processes to control access and use of [Agency] information resources. Access management incorporates role based access controls (RBAC), privileged user access, access definitions, roles, and profiles.
Policy	Access Control Policy And Procedures (AC 1) • [Agency] shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls. Account Management (AC 2) • [Agency] shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership. • [Agency] shall identify authorized users of information system and specify access rights. • [Agency] shall establish a process to enforce access requests to be approved by business/data owner (or delegate) prior to provisioning user accounts. • [Agency] shall authorize and monitor the use of guest/anonymous and temporary accounts, and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required. • [Agency] shall establish a process to notify relevant personnel (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change. • [Agency] shall remove or disable default user accounts and, if user accounts cannot be removed or disabled, they should be renamed. • Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default. • Access requests from users shall be recorded and follow the [Agency] established approval process. • [Agency] shall ensure that user access requests are approved by a business owner (or any other pre-approved role). • Privileged accounts (e.g., system / network administrators having root level access, database administrators), shall only be allowed after approval by an [Agency] information security officer and/or similarly designated role. The approval shall be granted to a limited number of individuals with the requisite skill, experience, business

need, and documented reason based on role requirements.

- [Agency] shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.
- [Agency] shall implement processes to enforce periodic user access reviews (e.g., semi-annual) to be performed by information / data owners or their assigned delegate(s) to ensure the following:
    - Access levels remain appropriate, based upon approvals;
    - Terminated employees do not have active accounts;
    - There are no group accounts, unless approved; and
    - There are no duplicate user identifiers.
- [Agency] shall review information system accounts within every one-hundred eighty (180) days and require annual certification.
- [Agency] shall regulate information system access and define security requirements for contractors, vendors, and other service providers.
- [Agency] shall establish procedures to administer privileged user accounts in accordance with a role-based access model.

Access Enforcement (AC 3)

- [Agency] shall enforce approved authorizations for logical access to information systems.
- [Agency] shall implement encryption as an access control mechanism if required by Federal, State or other laws or regulations.

Information Flow Enforcement (AC 4)

- For Restriced data: [Agency] systems shall enforce data flow controls using security attributes on information, source, and destination objects as a basis for flow control decisions.

Separation Of Duties (AC 5)

- [Agency] shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to:
    - Audit functions are not performed by security personnel responsible for administering information system access;
    - Divide critical business and information system management responsibilities;
    - Divide information system testing and production functions between different individuals or groups; and
    - Independent entity to conduct information security testing of information systems.
- [Agency] shall document and implement separation of duties through assigned information system access authorizations.

Least Privilege (AC 6)

- [Agency] shall ensure that only authorized individuals have access

to [Agency] data / information and that such access is strictly controlled, audited in accordance with the concepts of “need-to-know, least-privilege, and separation of duties”.

- [Agency] shall implement processes or mechanisms to:
  - Disable file system access not explicitly required for system, application, and administrator responsibilities;
  - Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors;
  - Restrict use of database management to authorized database administrators;
  - Grant access to authorized users based on their required job duties; and
  - Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password protected.

Unsuccessful Login Attempts (AC 7)

- [Agency] systems shall enforce a limit of unsuccessful logon attempts during an [Agency]-defined period. The number of logon attempts shall be commensurate with the classification of data hosted, processed or transferred by the information system.
- [Agency] shall automatically lock user accounts the after maximum logon attempts is reached. [Agency] shall establish an account lock time period commensurate with the classification of data hosted, processed or transferred by the information system.

System Use Notification (AC 8)

- [Agency] systems shall display the following warning before granting system access. “This system is solely for the use of authorized [Agency] personnel. The information contained herein is the property of [Agency] and subject to non-disclosure, security and confidentiality requirements. [Agency] shall monitor system usage for unauthorized activities. Any user accessing this system expressly consents to such monitoring.
- [Agency] implements warning banners that comply with Federal, State or other laws of regulations associated with the type of data handled by the [Agency] (e.g., For FTI IRS Publication 1075 requirements apply).

Session Lock (AC 11)

- [Agency] systems shall time out sessions or require a re-authentication process after (30) minutes of inactivity.

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: AC 1 Access Control Policy And Procedures NIST SP 800-53 Revision 4: AC 3 Access Enforcement NIST SP 800-53 Revision 4: AC 4 Information Flow Enforcement NIST SP 800-53 Revision 4: AC 5 Separation Of Duties

	NIST SP 800-53 Revision 4: AC-6 Least Privilege NIST SP 800-53 Revision 4: AC 7 Unsuccessful Login Attempts NIST SP 800-53 Revision 4: AC 8 System Use Notification NIST SP 800-53 Revision 4: AC 11 Session Lock
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Network Access Management

Purpose

The purpose of the network access management section is to establish procedures to control and monitor access and use of the network infrastructure. These are necessary to preserve the integrity, availability and confidentiality of [Agency] information.

Policy

Remote Access (AC 17)

- [Agency] shall document allowed methods for remote access to the network and information systems.
- [Agency] shall utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.
- Virtual Private Network (VPN) or equivalent encryption technology shall be used to establish remote connections with [Agency] networks and information systems.
- Remote users shall connect to [Agency] information systems only using mechanism protocols approved by the [Agency] through a limited number of managed access control points for remote connections.
- For Restricted data and/or system administrators: [Agency] employees and authorized third parties accessing [Agency] information systems remotely shall do so via an approved two-factor authentication (2FA) technology.
- [Agency] shall develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required).

Wireless Access (AC 18)

- [Agency] establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
- [Agency] shall only use wireless networking technology that enforces user authentication.
- [Agency] shall authorize wireless access to information systems prior to allowing use of wireless networks.
- [Agency] does not allow wireless access points to be installed independently by users.

Use of External Information Systems (AC 20)

- If external systems are authorized by the [Agency], the [Agency] shall establish terms and conditions for their use, including types of applications that can be accessed from external information systems, security category of information that can be processed, stored, and transmitted, use of VPN and firewall technologies, the use and protection against the vulnerabilities of wireless technologies, physical security maintenance and the security capabilities of installed software are to be updated.

	Boundary Protection (SC 7) • [Agency] networks where information deemed critical by [Agency] is stored or processed shall be physically or logically segregated from publicly available networks. • [Agency] networks and information systems shall not be accessible from pubic networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices. • [Agency] limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: AC 17 Remote Access NIST SP 800-53 Revision 4: AC 18 Wireless Access NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems NIST SP 800-53 Revision 4: SC 7 Boundary Protection
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Identity Management

Purpose	The purpose of the identity management section is to establish a standardized method to create and maintain verifiable user identifiers, and enable decisions about the levels of access to be given to each individual and/or groups.
Policy	Identification and Authentication (IA 2, IA 4 AND IA 8) • [Agency] shall establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators. • [Agency] shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier. • [Agency] shall allow the use of group IDs only where these are necessary for business or operational reasons; group IDs shall be formally approved and documented. • If [Agency] requires group IDs, it shall require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID). • [Agency] shall minimize the use of system, application, or service accounts; and [Agency] shall document, formally approve, and designate a responsible party of this type of accounts. • [Agency] security system shall be able to identify and verify the identification and, if deemed necessary by [Agency], the location of each authorized user.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users) NIST SP 800-53 Revision 4: IA 4 Identifier Management NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Authentication

Purpose	The purpose of the authentication section is to establish the authentication methods utilized by the [Agency] for authenticating, external / remote access connections, VPN access, administrative function access, vendor access and remote access to sensitive information.
Policy	Authenticator Management (IA 5) • [Agency] shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user. Unsuccessful Logon Attempts (AC 7) • [Agency] shall implement mechanisms to record successful and failed authentication attempts. Session Lock (AC 11) • [Agency] shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems. • [Agency] networks and information systems shall disable user access upon reaching the maximum number of invalid access attempts as defined by the [Agency]. • Network and information systems sessions should remain locked for a predetermined time or until the user reestablishes access through an established authentication procedure.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts NIST SP 800-53 Revision 4: AC 11 Session Lock NIST SP 800-53 Revision 4: IA 5 Authenticator Management
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.5 Emergency Access

Purpose	The purpose of the emergency access section is to establish conditions under which emergency access is granted, outlines rules to determine who is eligible to obtain emergency access and the authorized personnel entitled to grant access.

Policy	Account Management (AC 2)
	• [Agency] shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.
	• The emergency procedures shall ensure that:
	  ○ Only identified and authorized personnel are allowed access to live systems and data;
	  ○ All emergency actions are documented in detail; and
	  ○ Emergency action is reported to management and reviewed in an orderly manner.
	• [Agency] will establish a process to automatically terminate emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three-hundred sixty-five (365) days.

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: AC 2 Account Management
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.6 Password Policy

Purpose	The purpose of the password section is to establish uniform and enterprise-wide practices to create, manage and maintain passwords to ensure expected level of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

Policy	Account Management (AC 2)
	• [Agency] shall establish a process for password-based authentication to include the following:
	  ○ Automatically force users (including administrators) to change user account passwords every ninety (90) days. If [Agency] handles Restricted data, consider enforcing password changes no less than every sixty (60) days;
	  ○ Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every sixty (60) days;
	  ○ Passwords for system accounts to be changed at least every one hundred eighty (180) days;
	  ○ Enforce password minimum lifetime of one (1) day;
	  ○ Prohibit the use of dictionary names or words as passwords;
	  ○ Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters, and numbers) and/or special characters;
	  ○ Enforce a minimum number of characters to be changed when new passwords are created. For Restricted data consider a minimum of four (4) changed characters.
	  ○ Encrypt passwords in storage and during transmission;
	  ○ Prohibit password reuse for six (6) generations prior to reuse;
	  ○ For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account, every 60 days, at a minimum, for privileged users.
	• [Agency] users shall not share passwords with others under any circumstance.
	• System passwords shall be changed immediately upon termination / resignation of any employee with privileged access.
	• [Agency] shall not allow users to use common words or based on personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).
	• [Agency] shall suspend user accounts after a specified number of days of inactivity.

	• [Agency] shall implement a process to change passwords immediately if there reason to believe a password has been compromised or disclosed to someone other than the authorized user.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: AC 2 Account Management
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.7 Password Administration

Purpose	The purpose of the password administration section to ensure that the allocation of passwords is controlled through a formal management process.
Policy	Access Agreements (PS 6) • [Agency] users shall sign an acknowledgement to evidence understanding of authentication policies, including the [Agency] policy to keep passwords confidential and to keep group passwords solely within the members of the group. • [Agency] shall require that employees sign acknowledgement prior to allowing access to network and information systems. Identification and Authentication (IA 2, IA 6 and IA 8) • [Agency] shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password. • [Agency] shall establish a process to uniquely identify and authenticates non-Agency users. • [Agency] shall establish procedures to manage new or removed privileged accounts passwords Authenticator Management (IA 5) • First-time passwords shall be set to a unique value per user and changed immediately after first use. • [Agency] shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited. • [Agency] shall not allow default passwords for network and remote applications. Authenticator Feedback (IA 6) • [Agency] shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users) NIST SP 800-53 Revision 4: IA 5 Authenticator Management NIST SP 800-53 Revision 4: IA 6 Authenticator Feedback NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users) NIST SP 800-53 Revision 4: PS 6 Access Agreements
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Annual Certification: Process of reviewing user accounts to certify on behalf of the data/information owner that each user has a continuing need to access the application system, and that each user is entitled only to the privileges needed to perform current job duties.

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: Act of exposing the magnetic media to a strong magnetic field in order to disrupt the recorded magnetic data.

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.

Multifactor authentication: System authentication using two or more factors to achieve authentication, such as (i) something you know (e.g., password or PIN), (ii) something you have (e.g., token), (iii) something you are (e.g., biometric).

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.

Remote access: Any access to an information system by a user communicating through an external network (e.g., the Internet)

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.