DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Mobile Security

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

Mobile Security

1.1 Mobile Security

Purpose	The purpose of the mobile security section is to describe the minimum security policy for mobile devices used to access State data, including usage restrictions, configuration management, device authentication, and implementation of mandatory security software.
Policy	State business requirements may, on occasion, justify storing confidential data on mobile computing devices. It is the responsibility of the [Agency] to recognize the associated risks and take the necessary steps to protect and secure their mobile computing devices. Device Identification (MP 7) • [Agency] only allows portable media devices when these are assigned and identified to an individual owner. • [Agency] only allows the use of portable media devices that allow sanitization. • [Agency] shall use mobile devices that have the ability to be remotely wiped / erased. Access Control for Mobile Devices (AC 19) • [Agency] shall develop usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. • [Agency] shall develop a list of approved mobile devices. Only approved mobile devices shall be allowed to access the [Agency]'s network and information systems. • [Agency] shall develop and apply adequate asset management procedures to all mobile devices. • [Agency] shall utilize the approved encryption standard for mobile devices. • [Agency] shall implement controls to centrally manage the installation of standardized operating system, applications and patches on mobile devices. • [Agency] shall remove sensitive and confidential information from the mobile device before it is disposed. • [Agency] shall deploy administrative and technical controls to mitigate risks associated with lost or stolen mobile devices. • In order to reduce risks associated with vulnerabilities in mobile devices, [Agency] shall implement: ○ Controls for testing vendor recommended patches, hot-fixes or service packs before such changes are approved installation; and

	○ A process to keep system hardware, operating system and applications up-to-date with the approved system updates. • [Agency] shall disable all mobile device options and applications that are not in use or required by users' duties. • [Agency] shall protect all mobile devices with password or Personal Identification Number (PIN). • [Agency] shall ensure all mobile devices have timeout/locking features. • [Agency] shall develop controls for the protection of data storage on mobile devices including removable media. • [Agency] shall protect the storage and transmission of information on portable and mobile information devices through scanning the devices for malicious code, virus protection software. Before a mobile device is connected to an [Agency]'s network, it shall be scanned for viruses. If mobile device is used for transitional storage (e.g., copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion. • [Agency] shall develop a process for users to notify designated personnel when mobile devices are lost or stolen. The process shall include remote wiping / erasing of mobile devices. Access Agreements (PS 6) • [Agency] shall ensure that individuals requiring access to information or information systems sign appropriate access agreements prior to being granted access. • The physical security of these devices shall be the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out of-sight.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: Media Use NIST SP 800-53 Revision 4: AC 19 Access Control for Mobile Devices 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

1.2 Removable Media Security

Purpose	The purpose of the removable media security section is to establish security requirements and provide guidance to protect both the physical devices and the information they contain.
Policy	Media Protection Policy and Procedures (MP 1) • [Agency] shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures. Media Storage (MP 4) • For sensitive data, [Agency] shall physically control and securely store digital (e.g., CD, flash drives) and non-digital (e.g., paper) media within secured locations. • [Agency] shall ensure that only secure portable storage devices (e.g., encrypted flash drives) are utilized as removable media. Media Transport (MP 5) • [Agency] shall employ encryption mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. • [Agency] shall establish a process to enforce accountability for removable media during transport outside of controlled areas. Media Sanitization (MP 6) • [Agency] shall sanitize removable digital and non-digital media prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: MP 1 Media Protection Policy and Procedures NIST SP 800-53 Revision 4: MP 4 Media Storage NIST SP 800-53 Revision 4: MP 5 Media Transport 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 Portable Computing Devices

Purpose	The purpose of the Portable Computing Devices security section is to establish security mechanisms to protect both portable computing devices, such as laptops, and the information they contain.
Policy	Access Control for Mobile Devices (AC 19) • [Agency] shall employ whole disk encryption to protect the confidentiality and integrity of information stored on computing devices, including laptops. • [Agency] shall configure computing devices operating system (OS) so that only approved services are enabled and/or installed. • [Agency] shall implement a configuration management process that includes flaw remediation such as installing most current stable security patches, critical security updates and hot fixes for the relevant OS. • [Agency] shall implement tools to automatically update virus definition files on laptops and other portable computing devices susceptible to viruses. • [Agency] shall install firewall software on laptops and implement mechanisms that prevent users from making firewall configuration changes. • Unauthorized software shall not be installed on laptops and/or other portable computing devices. Approval shall be obtained for the installation of any software that may be required for business use. • [Agency] shall place asset tags on portable computing devices. • [Agency] shall disable Peer-to-Peer wireless connections, otherwise known as “Ad-Hoc Connections”, on all portable computing devices, including laptops.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: AC 19 Access Control for Mobile Devices
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: Act of 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.

Mobile Devices: A mobile device is a computing device that: (i) is portable so that it can easily be carried by a single individual; (ii) is designed to operate without a physical connection (e.g., wirelessly transmit or receive information); (iii) possesses local, non-removable or removable data storage; and (iv) includes a self-contained

power source.

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.