DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Threat and Vulnerability Management

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	Threat and Vulnerability Management	1.0	Initial draft
4/21/2014	Division of Information Security	Threat and Vulnerability Management	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

Threat and Vulnerability Management

1.1 Vulnerability Assessment

Purpose	The purpose of the Vulnerability Assessment policy is to establish controls and processes to help identify vulnerabilities within the [Agency] technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data.
Policy	Vulnerability Scanning (RA 5) • [Agency] shall implement processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems / applications are reported. • [Agency] shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports. • [Agency] shall analyze vulnerability scan reports and results from security control assessments. • [Agency] shall remediate identified vulnerabilities in accordance with [Agency] assessment of risk. Penetration Testing (CA 8) • [Agency] shall conduct penetration testing exercises on an annual basis, either by use of internal resources or employing an independent third party penetration team.
Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning NIST SP 800-53 Revision 4: CA 8 Penetration Testing
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Incident Management

Purpose

The purpose of the Incident Management policy is to establish controls and processes that will provide the [Agency] information system effective monitoring capability and responsiveness against security threats and incidents. Design and implementation of an incident management framework can secure the information system against known vulnerabilities and threats.

Policy

Incident Response Policy and Procedures (IR 1)

- [Agency] shall develop, document, and publish an incident response policy that addresses scope, roles, and responsibilities, internal coordination efforts, and compliance.
- [Agency] shall establish formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls.
- [Agency] shall review and update the incident response policy and procedures on an annual basis.

Incident Response Plan (IR 8)

- [Agency] shall develop and/or hire a third party vendor to implement an incident response plan to:
  - establish a roadmap for implementing incident response capabilities;
  - identifies and documents the requirements of the organization, including mission, size, structure, and functions;
  - define the types of information security incidents to be reported;
  - establish metrics to help ensure incident response capabilities remain effective; and
  - Define resources, such as technology and personnel, required to effectively support incident response capabilities.
- [Agency] shall review and update the incident response plan on an annual basis.

Incident Handling (IR 4)

- [Agency] shall implement formal processes to handle security incidents, including preparation, detection and analysis, containment, eradication, and recovery.
- [Agency] shall implement dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents.

Incident Monitoring and Reporting (IR 5, IR 6)

- [Agency] shall establish a process and tools to maintain detailed records of information security incidents that occur in external

(e.g., boundary systems) and internal information systems.

- [Agency] shall implement a policy to require personnel to report suspected information security incidents to the incident response team and/or [Agency] leadership.

Information System Monitoring (SI 4)

- [Agency] shall monitor information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.
- [Agency] shall deploy monitoring devices strategically within information technology environment to collect information security events and associated information.
- [Agency] shall protect information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
- [Agency] shall monitor inbound and outbound communications traffic to/ from the information system for unusual or unauthorized activities or conditions.
- [Agency] shall heighten the level of information system monitoring activity whenever there is an indication of increased risk to [Agency] operations, individuals and assets,

Incident Response Training (IR 2)

- [Agency] shall provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.
- [Agency] shall provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

Incident Response Testing (IR 3)

- [Agency] shall establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.
- [Agency] shall document the incident response test results and update incident response processes as applicable.

Malicious Code Protection (SI 3)

- [Agency] shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
- [Agency] shall implement a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.
- [Agency] shall configure malicious code protection mechanisms to perform periodic scans at defined time intervals.
- [Agency] shall block malicious code and send an alert to information system/networks administrator and initiate action(s) in response to malicious code detection.

Policy Supplement	Refer to the *Division of Information Security* website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: IR 1 Incident Response Policy and Procedures NIST SP 800-53 Revision 4: IR 2 Incident Response Training NIST SP 800-53 Revision 4: IR 3 Incident Response Testing NIST SP 800-53 Revision 4: IR 4 Incident Handling NIST SP 800-53 Revision 4: IR 5 Incident Monitoring NIST SP 800-53 Revision 4: IR 6 Incident Reporting NIST SP 800-53 Revision 4: IR 8 Incident Response Plan NIST SP 800-53 Revision 4: SI 3 Malicious Code Protection NIST SP 800-53 Revision 4: SI4 Information System Monitoring
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Patch Management

Purpose	The purpose of the Patch Management policy is to identify controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.
Policy	Flaw Remediation (SI 2) • [Agency] shall develop and implement a process to identify, report, and correct information system flaws. • [Agency] shall establish a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation. • [Agency] shall install latest stable versions of applicable security software and firmware updates. • [Agency] shall establish a patch cycle that guides the normal application of patches and updates to systems. • [Agency] shall establish a process of patch testing to verify the source and integrity of the patch and ensure testing in a production mirrored environment for a smooth and predictable patch roll out.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: SI 2 Flaw Remediation NIST SP 800-53 Revision 4: CM 2 Baseline Configuration
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.

Honeypot: A honeypot is set up as a decoy to attract adversaries and to deflect their attacks away from the operational systems supporting organizational missions/business function.

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.

Malicious Code: Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Malware: See *Malicious Code* definition.

Penetration Testing: A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of an information system.

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

Thin Node: Deployment of information system components having reduced/minimal functionality (e.g., diskless nodes and thin client technologies).

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

Vulnerability Analysis or Assessment: Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.