DIVISION OF INFORMATION SECURITY (DIS)

Information Security Policy – Business Continuity Management

Draft V0.1 – March 7, 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	Business Continuity Management	1.0	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. 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 to improve the security posture of the State and help safeguard [Agency] information technology resources. Agencies and institutions may leverage existing or develop new 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.

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

Business Continuity Management

1.1 Contingency Planning

Purpose	The purpose of the contingency planning section is to establish procedures and processes to maintain continuity of critical business operations during or post an incident. This section includes implementation of controls to identify and reduce risks, to limit the impact of damaging incidents, and to ensure the timely resumption of critical business operations.
Policy	Contingency Planning Policy and Procedures (CP 1) • [Agency] shall establish a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. • [Agency] shall establish formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls. • [Agency] shall establish a formal process for annual contingency planning policy and procedure review and update. Contingency Plan (CP 2, CP 7) • [Agency] shall conduct a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the [Agency] and determine a point in time (i.e. recovery time objective (RTO)) when the impact of an interruption or disruption becomes unacceptable to the [Agency]. • [Agency] shall utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications. • [Agency] shall assign contingency roles and responsibilities to key individuals from all business functions. • [Agency] shall establish procedures to maintain continuity of critical business functions despite critical information system disruption, breach, or failure. • [Agency shall document a Business Continuity Plan (BCP) that addresses documented recovery strategies designed to enable the [Agency] to respond to potential disruptions and recover its critical business functions within a predetermined RTO following a disruption. • [Agency] shall establish a process to ensure that the BCP is reviewed and approved by senior management. • [Agency] shall distribute copies of the BCP to key personnel responsible for the recovery of the critical business functions and other relevant personnel and partners with contingency roles, as

	determined by the [Agency]. • [Agency] shall establish and implement procedures to review the BCP at planned intervals and at least on an annual basis. • [Agency] shall establish a process to update the contingency plan, including BIA, when changes to the organization, information system, or environment of operation occurred. Contingency Training (CP 3) • [Agency] shall provide training to personnel with assigned contingency roles and responsibilities. • [Agency] shall establish a process for identifying and delivering training requirements (i.e., frequency) to and from the relevant participants and evaluating the effectiveness of its delivery. • [Agency] shall incorporate simulated events and lessons learned into contingency training to facilitate effective response by personnel with contingency roles when responding to disruption. Contingency Plan Testing (CP 4) • [Agency] shall test the BCP at least annually to determine the effectiveness of the plan and the [Agency's] readiness to execute the plan. • [Agency] shall review the BCP test results, record lessons learned and perform corrective actions as needed. • [Agency] shall employ standard testing methods, ranging from walk-through and tabletop exercises to more elaborate parallel/full interrupt simulations, to determine the effectiveness of the plan and to identify potential weaknesses in the plans. Criticality Analysis (SA 14) • n[Agency] shall establish procedures to enable continuation of critical business operations while operating in emergency mode.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: CP 1 Contingency Planning Policy and Procedures NIST SP 800-53 Revision 4: CP 2 Contingency Plan NIST SP 800-53 Revision 4: CP 3 Contingency Training NIST SP 800-53 Revision 4: CP 4 Contingency Plan Testing NIST SP 800-53 Revision 4: SA 14 Criticality Analysis
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Disaster Recovery and Contingency Strategies

Purpose

The purpose of the disaster recovery and contingency strategies section is to establish procedures to facilitate the recovery and restoration of [Agency] critical business functions in a timely manner by ensuring availability of requisite resources – work location, equipment and technology.

Policy

Disaster Recovery Plan (CP 2)

- [Agency] shall develop a Disaster Recovery Plan (DRP) that addresses scope, roles, responsibilities, and coordination among organizational entities for reallocating information systems operations to an alternate location.
- [Agency] shall establish recovery time objectives for the BIA identified critical information systems.
- [Agency] shall establish and document procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.
- [Agency] shall assign disaster recovery roles and responsibilities to key individuals.
- [Agency] shall establish a process to ensure that the DRP is reviewed and approved by senior management.
- [Agency] shall distribute copies of the DRP to key personnel responsible for the recovery of the critical information systems and other relevant personnel and partners with contingency roles, as determined by the [Agency].
- [Agency] shall establish and implement procedures to review the DRP at planned intervals and at least on an annual basis.
- [Agency] shall establish a process to update the DRP when changes to the organization or environment of operation occurred.

Alternate Site (CP 7)

- [Agency] shall identify and establish processes to relocate to an alternate site to facilitate the resumption of information system operations for business-critical functions within the defined recovery objectives (RTO and Recovery Point Objective (RPO)) when the primary site is unavailable due to disruption.
- [Agency] shall ensure that equipment and supplies required to resume operations at the alternate processing site are available.
- [Agency] shall ensure contracts are in place with third parties and suppliers to support delivery to the site within the defined time period for transfer/ resumption of critical business operations.
- [Agency] shall ensure that the alternate processing site provides information security safeguards similar to that of the primary site.
- [Agency] shall identify potential accessibility problems to the

alternate site in the event of an area-wide disruption or disaster.

Telecommunications Services (CP 8)

- [Agency] shall establish primary and alternate telecommunication service agreements with priority-of-service provisions in accordance with organizational availability requirements (including RTOs), quality of service and access;
- [Agency] shall establish alternate telecommunications services to facilitate the resumption of information system operations for critical business functions within the defined recovery objectives when the primary telecommunications capabilities are unavailable.
- [Agency] shall require primary and alternate telecommunication service providers to have contingency plans.

Information System Recovery and Reconstitution (CP 10)

- [Agency] shall establish documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.
- [Agency] shall implement procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
- [Agency] shall provide the capability to restore information system components within defined restoration time periods from configuration-controlled and integrity-protected information representing a known, operational state for the components (for e.g. reimaging methods).
- [Agency] shall establish measures to protect backup and restoration hardware, firmware, and software.

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: CP 7 Alternate Processing Site NIST SP 800-53 Revision 4: CP 8 Telecommunications Services NIST SP 800-53 Revision 4: CP 10 Information System Recovery and Reconstitution
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Data Backups

Purpose

The purpose of the Data Backup section is to establish procedures and processes to create and maintain information system data backup for easy storage and retrieval process in order to support the disaster recovery process.

Policy

Data Backup and Storage Policy

- [Agency] shall develop, maintain and document a Data Backup and Storage Policy that address the adequate procedures to storage data and thus ensure the recovery of electronic information in the event of failure.
- [Agency] shall identify and apply security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handle by the entity.

Alternate Storage Site (CP 6)

- [Agency] shall identify an alternate storage site that is separated from the primary site so as not to be susceptible to same hazards to storage and recover information system backup information.
- [Agency] shall establish necessary agreements with the site/ location owner to ensure that data storage and retrieval process are not hindered during or post an incident.
- [Agency] shall ensure that the alternate storage site provides information security safeguards similar to that of the primary storage site.
- [Agency] shall identify potential accessibility problems to the alternate storage site in the event of a disruption or disaster.
- [Agency] shall identify secure transfer methods when transporting backup media off-site.
- [Agency] shall establish and maintain an authorization list to retrieve backups from the off-site location.
- [Agency] shall review on an annual basis the security of the off-site location to ensure data is unexposed to unauthorized disclosure or modification while in storage.

Information System Backup (CP 9)

- [Agency] shall establish a process to perform data backups of user-level and system-level information at a defined frequency consistent with the established RTOs and RPOs.
- Agency] shall establish a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.
- [Agency] shall establish safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.
- [Agency] shall identify encryption/secure methods in storage of

	backup data to transportable media (i.e., tapes, CD Rooms, etc.) • [Agency] shall enforce dual authorization (“two-person control”) for the deletion or destruction of [Agency] sensitive data.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: CP 6 Alternate Storage Site NIST SP 800-53 Revision 4: CP 9 Information System Backup
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Incident: An event that has the potential to cause interruption, disruption, loss, emergency, crisis, disaster, or catastrophe.

Recovery: Activities and programs designed to return conditions to a level that is acceptable to the entity.

Response: The term response of an entity refers to the response of an entity to an incident or other significant event that might impact the entity. An incident response can include evacuating a facility, conducting damage assessment, initiating recovery strategies, and any other measures necessary to bring an entity to a more stable status.

Recovery Time Objective (RTO): The recovery time objective is the period of time within which systems, applications, or functions must be recovered after an outage (e.g., one business day). RTOs are often used as the basis for the development of recovery strategies and as a determinant as to whether to implement the recovery strategies during a disaster situation.

Recovery Point Objective (RPO): The recovery point objective is the point within a data flow that will be used as a base to begin the recovery of data back to the state at the time of disruption. The gap between the recovery point objective and the state at the time of disruption equals the data loss sustained during the incident.

Business Impact Analysis (BIA): An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption.