

South Carolina Workers' Compensation Commission

Information Security Policy – Asset Management

v1.0 – October 10, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/10//2014	Betsy Hartman	Director of IT	1.0	Initial Draft based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. OVERVIEW.....	4
INFORMATION SECURITY POLICY	5
<i>Asset Management</i>	5
1.1 <i>Asset Identification</i>	5
DEFINITIONS.....	7

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 South Carolina Workers’ Compensation Commission policies and federal and state regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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

Asset Management

1.1 Asset Identification

Purpose

The purpose of asset identification is to define the basis for developing an inventory of assets that support South Carolina Workers' Compensation Commission. Compiling an inventory of assets is important for judging the relative value and importance of agency assets. Based on this information, South Carolina Workers' Compensation Commission shall provide appropriate levels of protection.

Policy

Information System Component Inventory (CM 8)

- South Carolina Workers' Compensation Commission shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a system/business owner, a data classification, and a description of the location of the asset.
- Examples of assets associated with information systems are:
- **Information assets:** databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information;
 - **Software assets:** application software, system software, development tools and utilities;
 - **Physical assets:** physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks); and
 - **Services:** computing and communications services.
- Access to South Carolina Workers' Compensation Commission assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.
 - South Carolina Workers' Compensation Commission shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.

Security Impact Analysis (CM 4)

- South Carolina Workers' Compensation Commission shall classify assets into the data classification types in the State of South Carolina Data Classification Schema.
- South Carolina Workers' Compensation Commission shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: CM 4 Security Impact Analysis NIST SP 800-53 Revision 4: CM 8 Information System Component Inventory

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.

South Carolina Workers' Compensation Commission

Information Security Policy – Business Continuity Management

V0.1 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS Policies

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Business Continuity Management.....</i>	<i>5</i>
1.1 <i>Contingency Planning</i>	<i>5</i>
1.2 <i>Disaster Recovery and Contingency Strategies.....</i>	<i>8</i>
1.3 <i>Data Backups</i>	<i>11</i>
DEFINITIONS.....	13

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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers' Compensation Commission 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)

- South Carolina Workers’ Compensation Commission shall establish a formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
- South Carolina Workers’ Compensation Commission shall establish formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls.
- South Carolina Workers’ Compensation Commission shall establish a formal process for annual contingency planning policy and procedure review and update.

Contingency Plan (CP 2, CP 7)

- South Carolina Workers’ Compensation Commission shall conduct a Business Impact Analysis (BIA) to identify functions, processes, and applications that are critical to the South Carolina Workers’ Compensation Commission 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].
- South Carolina Workers’ Compensation Commission shall utilize the BIA results to determine potential impacts resulting from the interruption or disruption of critical business functions, processes, and applications.
- South Carolina Workers’ Compensation Commission shall assign contingency roles and responsibilities to key individuals from all business functions.
- South Carolina Workers’ Compensation Commission 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 South Carolina Workers’ Compensation Commission to respond to potential disruptions and recover its critical business functions

within a predetermined RTO following a disruption.

- South Carolina Workers' Compensation Commission shall establish a process to ensure that the BCP is reviewed and approved by senior management.
- South Carolina Workers' Compensation Commission 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].
- South Carolina Workers' Compensation Commission shall establish and implement procedures to review the BCP at planned intervals and at least on an annual basis.
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission shall provide training to personnel with assigned contingency roles and responsibilities.
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission shall test the BCP at least annually to determine the effectiveness of the plan and the [Agency's] readiness to execute the plan.
- South Carolina Workers' Compensation Commission shall review the BCP test results, record lessons learned and perform corrective actions as needed.
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission critical business functions in a timely manner by ensuring availability of requisite resources – work location, equipment and technology.

Policy

Disaster Recovery Plan (CP 2)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall establish recovery time objectives for the BIA identified critical information systems.
- South Carolina Workers' Compensation Commission shall establish and document procedures to fully restore critical information systems, post an incident, without deterioration of the security safeguards originally planned and implemented.
- South Carolina Workers' Compensation Commission shall assign disaster recovery roles and responsibilities to key individuals.
- South Carolina Workers' Compensation Commission shall establish a process to ensure that the DRP is reviewed and approved by senior management.
- South Carolina Workers' Compensation Commission 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].
- South Carolina Workers' Compensation Commission shall establish and implement procedures to review the DRP at planned intervals and at least on an annual basis.
- South Carolina Workers' Compensation Commission shall establish a process to update the DRP when changes to the organization or environment of operation occurred.

Alternate Site (CP 7)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall ensure that equipment and supplies required to resume

operations at the alternate processing site are available.

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall ensure that the alternate processing site provides information security safeguards similar to that of the primary site.
- South Carolina Workers' Compensation Commission shall identify potential accessibility problems to the alternate site in the event of an area-wide disruption or disaster.

Telecommunications Services (CP 8)

- South Carolina Workers' Compensation Commission 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;
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall require primary and alternate telecommunication service providers to have contingency plans.

Information System Recovery and Reconstitution (CP 10)

- South Carolina Workers' Compensation Commission shall establish documented procedures to restore and recover critical business activities from the temporary measures adopted to support normal business requirements after an incident.
- South Carolina Workers' Compensation Commission shall implement procedures for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.
- South Carolina Workers' Compensation Commission 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).
- South Carolina Workers' Compensation Commission 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	<p data-bbox="519 415 954 447">Data Backup and Storage Policy</p> <ul data-bbox="581 464 1482 772" style="list-style-type: none"> <li data-bbox="581 464 1482 625">• South Carolina Workers’ Compensation Commission 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. <li data-bbox="581 642 1482 772">• South Carolina Workers’ Compensation Commission shall identify and apply security requirements for protecting data backups based on the different types of data (sensitive, confidential, public) handle by the entity. <p data-bbox="519 783 911 814">Alternate Storage Site (CP 6)</p> <ul data-bbox="581 831 1482 1686" style="list-style-type: none"> <li data-bbox="581 831 1482 961">• South Carolina Workers’ Compensation Commission 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. <li data-bbox="581 978 1482 1108">• South Carolina Workers’ Compensation Commission 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. <li data-bbox="581 1125 1482 1213">• South Carolina Workers’ Compensation Commission shall ensure that the alternate storage site provides information security safeguards similar to that of the primary storage site. <li data-bbox="581 1230 1482 1318">• South Carolina Workers’ Compensation Commission shall identify potential accessibility problems to the alternate storage site in the event of a disruption or disaster. <li data-bbox="581 1335 1482 1423">• South Carolina Workers’ Compensation Commission shall identify secure transfer methods when transporting backup media off-site. <li data-bbox="581 1440 1482 1528">• South Carolina Workers’ Compensation Commission shall establish and maintain an authorization list to retrieve backups from the off-site location. <li data-bbox="581 1545 1482 1686">• South Carolina Workers’ Compensation Commission 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. <p data-bbox="519 1696 984 1728">Information System Backup (CP 9)</p> <ul data-bbox="581 1745 1482 1839" style="list-style-type: none"> <li data-bbox="581 1745 1482 1839">• South Carolina Workers’ Compensation Commission 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.

- South Carolina Workers' Compensation Commission shall establish a process to perform data backups of information system security documentation at a defined frequency consistent with RTOs and RPOs.
- South Carolina Workers' Compensation Commission shall establish safeguards and controls to protect the confidentiality, integrity, and availability of backup information at storage locations.
- South Carolina Workers' Compensation Commission shall identify encryption/secure methods in storage of backup data to transportable media (i.e., tapes, CD Rooms, etc.)
- South Carolina Workers' Compensation Commission shall enforce dual authorization ("two-person control") for the deletion or destruction of South Carolina Workers' Compensation Commission 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.

South Carolina Workers' Compensation Commission

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

v1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	Director of IT	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. OVERVIEW.....	4
INFORMATION SECURITY POLICY	5
<i>Human Resource (HR) and Security Awareness.....</i>	<i>5</i>
1.1 <i>Human Resource Compliance</i>	<i>5</i>
1.2 <i>Security Awareness Training</i>	<i>6</i>
DEFINITIONS.....	7

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 South Carolina Workers’ Compensation Commission policies and federal and state regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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	<p>Personnel Security Policy and Procedures (PE 1)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission 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. <p>Personnel Screening (PS 3) and Third-Party Personnel Security (PS 7)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission 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. <p>Personnel Termination (PS 4) and Transfer (PS 5)</p> <ul style="list-style-type: none"> Upon termination / transfer of employment for employees, termination of engagement for non-employees, or immediately upon request, personnel shall return to the South Carolina Workers' Compensation Commission all agency documents (and all copies thereof) and other agency property and materials in their possession or control. <p>Access Agreements (PS 6)</p> <ul style="list-style-type: none"> 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	<p>NIST SP 800-53 Revision 4: PE 1 Personnel Security Policy and Procedures</p> <p>NIST SP 800-53 Revision 4: PS 3 Personnel Screening</p> <p>NIST SP 800-53 Revision 4: PS 4 Personnel Termination</p> <p>NIST SP 800-53 Revision 4: PS 5 Personnel Transfer</p> <p>NIST SP 800-53 Revision 4: PS 6 Access Agreements</p> <p>NIST SP 800-53 Revision 4: PS 7 Third-Party Personnel Security</p>

1.2 Security Awareness Training

Purpose	<p>The purpose of security and awareness training is to define the information security training requirements for South Carolina Workers' Compensation Commission employees, contractors and third party users.</p>
Policy	<p>Security Awareness Training (AT 2) and Information Security Workforce (PM 13)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission management shall require employees, contractors and third party users to apply security in accordance with established policies and procedures of the organization. <p>Role-Based Security Training (AT 3)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission 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. <ul style="list-style-type: none"> ○ 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 South Carolina Workers' Compensation Commission 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). <p>Testing, Training, and Monitoring (PM 14)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission will appoint a cyber-security awareness training coordinator to manage training content, schedules and user training completion status. • The South Carolina Workers' Compensation Commission 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	<p>A policy supplement has not been identified.</p>
Guidance	<p>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</p>

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.

South Carolina Workers' Compensation Commission

Information Security Policy – IT Compliance

V1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	Director of IT	1.0	Based on DIS final policy

Table of Contents

PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>IT Compliance</i>	5
1.1 <i>Audit and Compliance Requirements</i>	5
1.2 <i>Information System Audit Considerations</i>	6
1.3 <i>Information Security Continuous Monitoring</i>	8
DEFINITIONS.....	9

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 South Carolina Workers' Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers' Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers' Compensation Commission 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

IT Compliance

1.1 Audit and Compliance Requirements

Purpose	The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance of with information security policies and standards at State agencies and institutions.
Policy	<p>Compliance with legal and contractual requirements (A.15.1)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall identify and document its obligations to applicable State, federal and other third party laws and regulations in relation to information security. <p>Compliance with security policies and standards (A.15.2.1, A.15.2.2)</p> <ul style="list-style-type: none"> At least annually, South Carolina Workers' Compensation Commission shall perform reviews or audits of users' and systems' compliance with security policies, standards, and procedures, and initiate corrective actions where necessary. Results from compliance reviews or audits shall be documented, and reported to South Carolina Workers' Compensation Commission leadership. <p>Audit and Accountability Policy and Procedures (AU 1)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall establish a formal, documented audit and accountability policy and associated audit and accountability procedures. South Carolina Workers' Compensation Commission shall implement a process to review and update the audit and accountability policy and associated procedures at least annually.
Policy Supplement	A policy supplement has not been identified.
Guidance	<p>ISO 27001:2005: A.15.1 Compliance with legal and contractual requirements</p> <p>ISO 27001:2005: A.15.2.1 Compliance with security policies and standards</p> <p>ISO 27001:2005: A.15.2.2 Technical compliance checking</p> <p>NIST SP 800-53 Revision 4: AU 1 Audit and Accountability Policy and Procedures</p>
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Information System Audit Considerations

Purpose

The purpose of the IS Audit Considerations section is to establish controls and processes to maximize the effectiveness of and to minimize interference to/from the information systems audit process.

Policy

Information systems audit controls (A.15.3.1)

- South Carolina Workers' Compensation Commission shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.

Protection of information systems audit tools (A.15.3.2)

- South Carolina Workers' Compensation Commission shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools.

Audit Events (AU 2)

- South Carolina Workers' Compensation Commission shall determine the type of events that are to be audited within information systems.
- South Carolina Workers' Compensation Commission shall review and update the list of audited events annually.
- South Carolina Workers' Compensation Commission leadership shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.

Content of Audit Records (AU 3)

- South Carolina Workers' Compensation Commission information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event.

Audit Records Review and Reporting (AU 6)

- South Carolina Workers' Compensation Commission shall analyze information system audit records periodically.
- South Carolina Workers' Compensation Commission shall report findings of audit records reviews to information security personnel and South Carolina Workers' Compensation Commission leadership.
- South Carolina Workers' Compensation Commission shall perform correlation and analysis of information generated by security assessments and monitoring.

Audit Storage Capacity (AU 4)

- South Carolina Workers' Compensation Commission shall allocate sufficient audit storage capacity to help ensure
-

	<p>compliance with audit logs retention requirements from State, federal, and other applicable third party laws and regulations.</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.
Policy Supplement	A policy supplement has not been identified.
Guidance	ISO 27001:2005: A.15.3.1 Information systems audit controls ISO 27001:2005: A.15.3.2 Protection of information systems audit tools NIST SP 800-53 Revision 4: AU 2 Audit Events NIST SP 800-53 Revision 4: AU 3 Content of Audit Records NIST SP 800-53 Revision 4: AU 4 Audit Storage Capacity NIST SP 800-53 Revision 4: AU 6 Audit Review, Analysis, and Reporting
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Information Security Continuous Monitoring

Purpose	The purpose of the Information Security Continuous Monitoring policy is to establish controls that will provide State agencies and institutions the effective monitoring and response capabilities in relation to compliance issues and incidents.
Policy	<p>Continuous Monitoring (CA 2)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall employ assessment teams to monitor the security controls on an ongoing basis. • South Carolina Workers' Compensation Commission assessment teams shall be independent from operational or business functions, or hired third parties. <p>Plan of Action and Milestones (CA 5)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as result of internal/external risk assessments, security reviews, and/or audits. • South Carolina Workers' Compensation Commission shall update its plan of action and milestones at least on a yearly basis, and also based on the findings from continuous security monitoring activities.
Policy Supplement	A policy supplement has not been identified.
Guidance	<p>NIST SP 800-53 Revision 4: CA 2 Security Assessments</p> <p>NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones</p>
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Auditable event: A system activity identified by the entity's audit monitoring system that may be indicative of a violation of security policy. The activity may range from simple browsing to attempts to plant a Trojan horse or gain unauthorized access privilege.

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.

Chief Information Officer: The agency official responsible for ensuring agency compliance with, and prompt, efficient, and effective implementation of, information policies and information resources management responsibilities, including information security and the management of information technology.

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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

Information System: A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Information System Owner: Official responsible for the overall procurement, development, integration, modification, or operation and maintenance of an information system.

South Carolina Workers' Compensation Commission

Information Security Policy – IT Risk Strategy

V0.1 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>IT Risk Strategy.....</i>	<i>5</i>
1.1 <i>Security Performance and Metrics</i>	<i>5</i>
1.2 <i>Third Party Risk Management</i>	<i>6</i>
DEFINITIONS.....	8

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.

This policy, along with other information security policies released by the Division of Information Security (DIS), provides 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 statewide information security policies, procedures, and recommended technology solutions
- Providing technical assistance, advice, and recommendations concerning information security matters

(B) Agency/Institution

Information security is a 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, including but not limited to updating agency/institution local policies, standards, and procedures to adopt
- Implementing and maintaining an Information Security Program
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency information security program
- Ensuring that security is part of the information planning and procurement process
- Participating in annual information systems data security self-assessments focusing on compliance to this State information security policies
- 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
- Implement security policies and procedures to help ensure 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 South Carolina Workers' Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers' Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers' Compensation Commission 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 relation 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

IT Risk Strategy

1.1 Security Performance and Metrics

Purpose	The purpose of the Security Performance and Metrics section is to establish controls to assess the performance of the security program and its components.
Policy	<p>Information Security Measures of Performance (PM 6)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall develop, monitor, and report on performance metrics to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program. [Agency]-defined performance measures should be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement. <p>Manageability of Metrics (3.4.2)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall ensure that the metrics/ measures that are collected are meaningful, yield impact and outcome findings, and provide stakeholders with the time necessary to use the results to address performance gaps. <p>Data Management Concerns (3.4.3)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.
Policy Supplement	A policy supplement has not been identified.
Guidance	<p>NIST SP 800-53 Revision 4: PM 6 Information Security Measures of Performance</p> <p>NIST SP 800-55 Revision 1: 3.4.2 Manageability</p> <p>NIST SP 800-55 Revision 1: 3.4.3 Data Management Concerns</p>
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Third Party Risk Management

Purpose	The purpose of the Third Party Risk Management section is to establish the controls to safeguard South Carolina Workers' Compensation Commission information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.
Policy	<p>External Information System Services (SA 9)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall establish a policy and associated processes to enforce that third parties comply with information security requirements and employ defined security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.• South Carolina Workers' Compensation Commission shall implement processes, methods, and techniques to monitor security control compliance by third parties on an ongoing basis. <p>Risk Assessment (RA 3)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall establish a process to conduct risk assessments on third party service providers, and document the risk assessment results.• South Carolina Workers' Compensation Commission shall implement controls to help ensure that risk assessments are updated in case of major changes in scope of services or contractual changes with third parties. <p>System Interconnections (CA 3)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall authorize connections from South Carolina Workers' Compensation Commission information systems to third party information systems by entering into Interconnection Security Agreements.• For each third party interface, South Carolina Workers' Compensation Commission shall document the interface characteristics, security requirements, and the nature of the information communicated. <p>Use of External Information Systems (AC 20)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall establish terms and conditions for trust relationships established with other entities owning, operating, and/or maintaining external information systems.• Terms and conditions established by South Carolina Workers' Compensation Commission should control:<ul style="list-style-type: none">○ Access to South Carolina Workers' Compensation Commission information systems from third party information systems; and○ Controls for processing, storing, or transmit of South

Carolina Workers' Compensation Commission data using third party information systems.

- South Carolina Workers' Compensation Commission shall review and update third party security agreements on an annual basis, or as defined in the contract.

Information Sharing with Third Parties (UL 2)

- South Carolina Workers' Compensation Commission shall share personally identifiable information (PII) with third parties only for the authorized purposes identified in the Privacy Act and/or described in its notice(s), as well as State laws and Interconnection Security Agreements.
- South Carolina Workers' Compensation Commission shall, where appropriate, enter into Memoranda of Understanding, Memoranda of Agreement, Letters of Intent, Computer Matching Agreements, or similar agreements, with third parties that specifically describe the types of sensitive data covered (e.g., PII) and specifically enumerate the purposes for which the data may be used.
- South Carolina Workers' Compensation Commission shall monitor, audit, and train its staff on the authorized sharing of sensitive data with third parties and on the consequences of unauthorized use or sharing of such data.
- South Carolina Workers' Compensation Commission shall evaluate any proposed new instances of sharing sensitive data with third parties to assess whether the sharing is authorized and whether additional or new public notice is required.

Policy Supplement

A policy supplement has not been identified.

Guidance

NIST SP 800-53 Revision 4: AC 20 Use of External Information Systems
 NIST SP 800-53 Revision 4: CA 3 System Interconnections
 NIST SP 800-53 Revision 4: PS 6 Access Agreements
 NIST SP 800-53 Revision 4: RA 3 Risk Assessment
 NIST SP 800-53 Revision 4: SA 9 External Information System Services
 NIST SP 800-53 Revision 4: UL 2 Information Sharing with Third Parties

Reference

http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Authentication: Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

Authorization (to operate): The official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other agencies, and the State based on the implementation of an agreed-upon set of security controls.

Developer: A general term that includes: (i) developers or manufacturers of information systems, system components, or information system services; (ii) systems integrators; (iii) vendors; (iv) and product resellers. Development of systems, components, or services can occur internally within organizations (i.e., in-house development) or through external entities.

Enterprise Architecture: A strategic information asset base, which defines the mission; the information necessary to perform the mission; the technologies necessary to perform the mission; and the transitional processes for implementing new technologies in response to changing mission needs; and includes a baseline architecture; a target architecture; and a sequencing plan.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

Metrics: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Personally Identifiable Information: Information which can be used to distinguish or trace the identity of an individual (e.g., name, social security number, biometric records, etc.) alone, or when combined with

other personal or identifying information which is linked or linkable to a specific individual (e.g., date and place of birth, mother's maiden name, etc.).

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other agencies, and the State.

Risk Assessment: The process of identifying risks to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place.

Safeguards: Protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices.

Security Control: A safeguard or countermeasure prescribed for an information system or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements.

Sensitive Data: Refers to information protected by State and/or federal law as well as data protected by Agency policies. Following are some prominent examples of sensitive data. Often, context plays a role in data sensitivity; thus, this list is not exhaustive: Social Security number (SSN), credit card number or banking information, passport number, tax information, and credit reports, among others.

System Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Trustworthiness (Information System): The degree to which an information system (including the information technology components that are used to build the system) can be expected to preserve the confidentiality, integrity, and availability of the information being processed, stored, or transmitted by the system across the full range of threats. A trustworthy information system is a system that is believed to be capable of operating within defined levels of risk despite the environmental disruptions, human errors, structural failures, and purposeful attacks that are expected to occur in its environment of operation.

South Carolina Workers' Compensation Commission

Information Security Program Master Policy

V1.0 - October 17, 2014

Revision History

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. SECTION OVERVIEW	4
PART 4. IMPLEMENTATION TIMELINE	5
INFORMATION SECURITY POLICY	6
<i>Governance</i>	6
1.1 <i>Information Security Program Planning</i>	6
1.2 <i>Security Organization (Roles and Responsibilities)</i>	8
1.3 <i>Policy Management (Plan of Action)</i>	9
1.4 <i>Information Security Controls Deployment</i>	11
DEFINITIONS.....	12

INTRODUCTION

Part 1. Preface

The South Carolina Information Security (Infosec) Program consists of information security policies, procedures, and other guidance that establish a common information security framework across South Carolina State Government Agencies.

Together these policies provide a framework for developing a state government agency's information security plan. An effective information security plan improves the State's security posture and aligns information security with an agency's mission, goals, and objectives.

Each agency's implementation of the Infosec Program must comply with the policy framework established by the SC DIS, as published in the *Policies* section of its website: <http://dis.sc.gov/PoliciesAndProcedures/Pages/default.aspx>.

Part 2. Organizational and Functional Responsibilities

This section sets the minimum level of responsibility for the following individuals and/or groups:

- Division of Information Security
- State Government Agencies
- 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
- Coordinating information security incident response for any incidents involving state government agencies

(B) State Government Agencies

Information security is a state government agency's responsibility shared by all members of the agency's management team. The management team shall provide clear direction and visible support for security initiatives. Each agency is responsible for:

- Initiating measures to assure and demonstrate compliance with the security requirements outlined in this policy
- Implementing and maintaining an Information Security Plan compliant with the SC DIS Information Security Program
- Identifying a role (position/person/title) that is responsible for implementing and maintaining the agency's information security plan
- Ensuring that security is part of the information systems planning and procurement process
- Participating in annual information systems data security self-audits ensuring that the agency's own practices are in compliance with the agency's Information Security Plan, and with the SC DIS Information Security Program

- 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 of the agency's information while it is being processed, stored, and/or transmitted electronically, and the security of the resources associated with those processing functions
- Ensuring that agency staff work with SC DIS and/or SC Enterprise Privacy Office (EPO) staff in resolving the agency's security and privacy incidents
- Ensuring separation of duties and assigning appropriate system permissions and responsibilities for the agency's system users
- Identifying 'business owners' for any new system, who are responsible for:
 - Classifying data according to the criteria published by SC DIS or SC EPO
 - 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
- Responsible for using information resources only for intended purposes as defined by policies, laws and regulations of the State or agency
- Accountable for their actions relating to their use of all State information systems

Part 3. 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).

Part 4. Implementation Timeline

Each state government agency should observe the following timeline in implementation of the Information Security Program. Exceptions must be reported to the office of the SC DIS Chief Information Security Officer.

Section	Implementation Date
1.1 Information Security Program Planning	30-Jun-2014
1.2 Security Organization (Roles and Responsibilities)	30-Jun-2014
1.3 Policy Management (Plan of Action)	31-Jan-2015
1.4 Information Security Controls Deployment	1-July-2016

INFORMATION SECURITY POLICY

Governance

1.1 Information Security Program Planning

Purpose

The purpose of this section is to establish the principles to regulate how agencies shall provide an appropriate level of governance controls over Information Security related activities.

Policy

Information Security Plan (PM 1)

- Each agency shall develop and communicate an information security plan that underlines security requirements, the security management controls, and common controls in place for meeting those requirements.
- Each agency's security plan shall identify and assign security program roles, responsibilities and management commitment, and ensure coordination among the agency's business units, as well as compliance with the security plan.
- Each agency shall ensure coordination among the agency's business units responsible for the different aspects of information security (i.e., technical, physical, personnel, etc.)
- Each agency shall ensure that the security plan is approved by senior management.
- Each agency shall review the information security plan at least on an annual basis.
- Each agency shall update the security plan to address changes and problems identified during plan implementation or security control assessments.
- Each agency shall protect the information security plan from unauthorized disclosure and modification.

Information Security Resources (PM 3)

- Each agency shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.

Plan of Action and Milestones Process (PM 4)

- Each agency shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.
- Each agency shall review plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

Information Security Measures of Performance (PM 6)

- Each agency shall develop, monitor, and report on the results of information security measures of performance, as directed or

	guided by the SC DIS and SC EPO.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PM 1 Information Security Program Plan NIST SP 800-53 Revision 4: PM 3 Information Security Resources NIST SP 800-53 Revision 4: PM 4 Plan of Action and Milestones Process NIST SP 800-53 Revision 4: PM 6 Measures of Performance
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Security Organization (Roles and Responsibilities)

Purpose	The purpose of this section is to establish key principles based on which each Agency's Security Organization shall be established.
Policy	<p>Information Security Authority (2.2.3.1)</p> <ul style="list-style-type: none"> Each agency's chief executive shall ensure that the agency's senior officials are given the necessary authority to secure the operations and assets under their control. <p>Information Security Liaison (PM 2)</p> <ul style="list-style-type: none"> Each agency shall appoint an information security liaison with the mission and resources to: coordinate, develop, implement, and maintain an information security plan. <p>Information Security Workforce (PM 13)</p> <ul style="list-style-type: none"> Each agency shall establish an information security workforce and professional development program appropriately sized to the agency's information security needs. <p>Role-based Security Training (AT 3)</p> <ul style="list-style-type: none"> Each agency shall provide role-based security training to personnel with assigned security roles and responsibilities.
Policy Supplement	A policy supplement has not been identified.
Guidance	<p>NIST SP 800-53 Revision 4: PM 2 Senior Information Security Officer</p> <p>NIST SP 800-53 Revision 4: PM 13 Information Security Workforce</p> <p>NIST SP 800-53 Revision 4: AT 3 Role-based Security Training</p> <p>NIST SP 800-100: 2.2.3.1 Agency Head</p>
Reference	<p>http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</p> <p>http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf</p>

1.3 Policy Management (Plan of Action)

Purpose	The purpose of this section is to establish key principles based on which each agency's security procedures shall be developed.
Policy	<p>Procedure Development</p> <ul style="list-style-type: none">• Each agency shall adopt a risk-based approach to identify State and agency-specific information security objectives, and shall develop information security procedures in alignment with the identified security objectives.• Each agency shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.• Each agency shall approach independent external (third party) specialists to assist in the development of information security policies in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency.• Each agency shall work in collaboration with other states, Federal government, and external special interest groups in cases where procedures directly or indirectly affect interfacing activities with them.• Information security procedures that are developed at the agency shall contain the following information, as appropriate:<ul style="list-style-type: none">○ Revision history○ Introduction○ Preface○ Ownership, roles, and responsibilities○ Purpose○ Policy statements○ Policy supplement○ Guidance○ Definitions• Scenarios which cannot be effectively addressed within the constraints of the agency's security procedures, should be identified as exceptions:<ul style="list-style-type: none">○ Exceptions shall be evaluated in the context of potential risk to the agency as a whole;○ Exceptions that create significant risks without adequate compensating controls shall not be approved; and○ Exceptions shall be consistently evaluated in accordance with the agency's risk acceptance practice.• Each agency shall review each draft procedure with stakeholders who shall be impacted by the procedure, to ensure that the procedure is enforceable and effective.

-
- Each agency shall identify gaps within the procedures that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps.
 - Each agency shall develop and implement a communication plan to disseminate new procedures or changes to existing procedures.
 - Each agency shall review procedures on an annual basis to ensure that procedures are up-to-date and aligned with the State’s risk posture.

Procedure Review and Approval

- A procedure governance committee shall be established for the purpose of review and approval of procedures.
- Procedure exemptions shall be explicitly approved by the procedure governing committee.
- Procedure approval history shall be documented in detail.

Procedure Implementation

- Each agency shall implement mechanisms to help ensure that information security procedures will be available to the agency’s personnel on a continuous basis and whenever required.
- Each agency shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PM 6 Measures of Performance
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Information Security Controls Deployment

Purpose	The purpose of this section is to establish key principles for deployment of information security controls.
Policy	<p>Controls Deployment</p> <ul style="list-style-type: none"> • Each agency shall adopt a risk-based approach to prioritize deployment of controls. • Each agency shall allocate the appropriate subject matter experts to the deployment of State and agency-specific information security controls. • Each agency shall approach independent external (third party) specialists to assist in the deployment of information security controls in cases where it is established that the required skills do not exist within the agency and are not available within any other state government agency. • Controls which cannot be deployed due to the agency's resource or other constraints must be reported to the office of the State Chief Information Security Officer. • Each agency shall review each control with stakeholders who shall be impacted, to ensure that the control is enforceable and effective. • Each agency shall identify gaps within the controls that are not enforceable and effective, shall document the gaps, and shall assign the appropriate resources to remediate the gaps. • Each agency shall develop and implement a communication plan to disseminate new controls or changes to existing controls. • Each agency shall review controls on an annual basis to ensure that they are up-to-date and aligned with the State's risk posture.
Policy Supplement	A policy supplement has not been identified.
Guidance	Guidance has not been identified.
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

DEFINITIONS

Agency, State Government – refers to any South Carolina state agency, institution, department, division, board, commission, or authority.

Control, Information Security – refers to any process or technology intended to reduce a security risk.

Guidance: Guidance refers to best practices and industry standards that have been used as a guide to develop the security policies and the policy supplements.

Information security liaison: Official responsible for carrying out the “Chief Information Officer” responsibilities within the agency under the Federal Information Security Management Act (FISMA) and serving as the primary liaison between the DIS office of the Chief Information Security Officer and the agency’s authorizing officials, information system owners, and information system security officers.

Information Security Plan – the collection of procedures and other guidance developed by state government agencies to implement the SC DIS Information Security Program within the agency

Metrics: Tools designed to facilitate decision making and improve performance and accountability through collection, analysis, and reporting of relevant performance-related data.

Policy: The Information Security Policy defines appropriate controls to protect an agency’s information assets from unauthorized disclosure, misuse, alteration, or destruction in a manner that ensures compliance with regulatory requirements and risk management expectations.

Policy supplement: Policy supplement assists the agencies in the actual implementation of the high level security controls defined in the policy. This defines at a granular level the baseline security controls for the agency.

Policy exemptions: Scenarios which require exemption from the existing provisions of the Security policy are called policy exemptions.

Risk posture: Risk posture identifies the specific threats that the agency faces and quantifies the risks associated with each of those threat events materializing.

SC DIS – South Carolina Division of Information Security

SC DIS Information Security Program – the collection of policies, procedures, and other guidance published on the SC DIS website (dis.sc.gov).

Standards: Security baseline to assist agencies, used to maintain a minimum baseline security configuration level as per industry guidelines.

System Security Plan: Formal document that provides an overview of the security requirements for an information system and describes the security controls in place or planned for meeting those requirements.

Information Security Policy – Physical & Environmental Security

V1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Physical & Environmental Security.....</i>	<i>5</i>
1.1 <i>Physical Access and Security.....</i>	<i>5</i>
1.2 <i>Environmental Security</i>	<i>8</i>
1.3 <i>Disposal of Equipment.....</i>	<i>10</i>
DEFINITIONS.....	11

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 South Carolina Workers’ Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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

Physical & Environmental Security

1.1 Physical Access and Security

Purpose

The purpose of the Physical Access and Security section is to establish controls to prevent unauthorized physical access to South Carolina Workers' Compensation Commission information assets to protect them from damage, interruption, misuse, destruction and/ or theft.

Policy

Physical and Environmental Protection Policy and Procedures (PE 1)

- South Carolina Workers' Compensation Commission shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
- South Carolina Workers' Compensation Commission shall establish procedures to review and maintain current the physical and environmental protection policy and associated procedures.

Physical Access Authorizations (PE 2)

- South Carolina Workers' Compensation Commission shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
- South Carolina Workers' Compensation Commission shall establish a process to review, approve, and issue credentials for facility access.
- South Carolina Workers' Compensation Commission shall remove individuals from the facility access list when access is no longer required.

Physical Access Control (PE 3)

- South Carolina Workers' Compensation Commission control entry to / exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/ or security guard(s).
- South Carolina Workers' Compensation Commission shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
- South Carolina Workers' Compensation Commission shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
- South Carolina Workers' Compensation Commission shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.
- South Carolina Workers' Compensation Commission shall establish

a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.

- South Carolina Workers’ Compensation Commission shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.

Access Control for Transmission Medium (PE 4)

- South Carolina Workers’ Compensation Commission shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).

Access Control for Output Devices (PE 5)

- South Carolina Workers’ Compensation Commission shall place output devices in secured areas and in locations that can be monitored by authorized personnel, and allow access to authorized individuals only.
- South Carolina Workers’ Compensation Commission shall control physical access to information system output devices (e.g., printers, copiers, scanners, facsimile machines) to prevent unauthorized individuals from obtaining sensitive data.

Monitoring Physical Access (PE 6)

- South Carolina Workers’ Compensation Commission shall review physical access logs at a defined frequency and upon occurrence of security incidents.

Visitor Access Records (PE 8)

- South Carolina Workers’ Compensation Commission shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of 1 year.

Delivery and Removal (PE 16)

- South Carolina Workers’ Compensation Commission shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

Policy Supplement

A policy supplement has not been identified.

Guidance

NIST SP 800-53 Revision 4: PE 1 Physical and Environmental Protection Policy and Procedures
 NIST SP 800-53 Revision 4: PE 2 Physical Access Authorizations
 NIST SP 800-53 Revision 4: PE 3 Physical Access Control
 NIST SP 800-53 Revision 4: PE 4 Access Control for Transmission Medium
 NIST SP 800-53 Revision 4: PE 5 Access Control for Output Devices
 NIST SP 800-53 Revision 4: PE 6 Monitoring Physical Access
 NIST SP 800-53 Revision 4: PE 8 Visitor Access Records
 NIST SP 800-53 Revision 4: PE 16 Delivery and Removal

Reference

N/A

1.2 Environmental Security

Purpose	The purpose of the Environmental Security section is to define controls to protect South Carolina Workers' Compensation Commission information assets from damage, destruction and/ or interruption due to environmental factors such as fire, humidity, water, power outage, etc.
Policy	<p>Power Equipment and Cabling (PE 9)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction. <p>Emergency Shutoff (PE 10)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall make available the capability of shutting off power to data center(s) during an incident.• South Carolina Workers' Compensation Commission shall place emergency shutoff switches or devices at locations which can be safely and easily accessed by personnel during an incident.• South Carolina Workers' Compensation Commission shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation. <p>Data Center Emergency Power (PE 11)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss. <p>Data Center Fire Protection (PE 13)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall install and maintain fire detection and suppression devices that are supported by an independent power source.• South Carolina Workers' Compensation Commission shall employ fire detection devices/ system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.• South Carolina Workers' Compensation Commission shall employ an automatic fire suppression system if/ when the data center(s) is not staffed on a continuous basis. <p>Data Center Temperature and Humidity Controls (PE 14)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.• South Carolina Workers' Compensation Commission shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment. <p>Data Center Water Damage Protection (PE 15)</p>

	<ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall protect processing equipment from damage resulting from water leakage.
Policy Supplement	A policy supplement has not been identified.
Guidance	NIST SP 800-53 Revision 4: PE 9 Power Equipment and Cabling NIST SP 800-53 Revision 4: PE 10 Emergency Shutoff NIST SP 800-53 Revision 4: PE 11 Emergency Power NIST SP 800-53 Revision 4: PE 13 Fire Protection NIST SP 800-53 Revision 4: PE 14 Temperature and Humidity Controls NIST SP 800-53 Revision 4: PE 15 Water Damage Protection
Reference	N/A

1.3 Disposal of Equipment

Purpose	<hr/> <p>The purpose of the Disposal of Equipment section is to define the controls that shall be followed for disposal of information system equipment which contains South Carolina Workers' Compensation Commission information.</p> <hr/>
Policy	<p>Media Sanitization (MP 6)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall define and implement mechanisms for disposal of digital media and data storage devices.• South Carolina Workers' Compensation Commission shall employ sanitization mechanisms with the strength and integrity commensurate with classification of data to be sanitized.• South Carolina Workers' Compensation Commission shall establish processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.• South Carolina Workers' Compensation Commission shall implement controls to track and verify sanitization of devices prior to disposal. <hr/>
Policy Supplement	<p>A policy supplement has not been identified.</p> <hr/>
Guidance	<p>NIST SP 800-53 Revision 4: MP 6 Media Sanitization</p> <hr/>
Reference	<p>N/A</p> <hr/>

DEFINITIONS

Audit Log: A chronological record of information system activities, including records of system accesses and operations performed in a given period.

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.

Availability: Ensuring timely and reliable access to and use of information.

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

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

Event: Any observable occurrence in an information system.

Incident: An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

Integrity: Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

Media: Physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within an information system.

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.

Risk: A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence.

Sensitive facilities: Refers to facilities use to store or process sensitive data in physical format (e.g., hard copy documents, tapes, computer equipment containing data) or digital media (e.g., warehouse with computer equipment, hard drives).

Sensitive Data: Refers to information protected by State and/or federal law as well as data protected by Agency policies. Following are some prominent examples of sensitive data. Often, context plays a role in data sensitivity; thus, this list is not exhaustive: Social Security number (SSN), credit card number or banking information, passport number, tax information, and credit reports, among others.

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

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

South Carolina Workers' Compensation Commission

Information Security Policy – Threat and Vulnerability Management

V1.0 – October 10, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/10/2014	Betsy Hartman	Director of IT	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Threat and Vulnerability Management</i>	<i>5</i>
1.1 <i>Vulnerability Assessment.....</i>	<i>5</i>
1.2 <i>Incident Management</i>	<i>6</i>
1.3 <i>Patch Management</i>	<i>9</i>
DEFINITIONS.....	10

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 South Carolina Workers’ Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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 South Carolina Workers' Compensation Commission 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	<p>Vulnerability Scanning (RA 5)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission 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. • South Carolina Workers' Compensation Commission shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports. • South Carolina Workers' Compensation Commission shall analyze vulnerability scan reports and results from security control assessments. • South Carolina Workers' Compensation Commission shall remediate identified vulnerabilities in accordance with South Carolina Workers' Compensation Commission assessment of risk. <p>Penetration Testing (CA 8)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission 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	<p>NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning</p> <p>NIST SP 800-53 Revision 4: CA 8 Penetration Testing</p>
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 South Carolina Workers' Compensation Commission 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)

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

Incident Response Plan (IR 8)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall review and update the incident response plan on an annual basis.

Incident Handling (IR 4)

- South Carolina Workers' Compensation Commission shall implement formal processes to handle security incidents, including preparation, detection and analysis, containment, eradication, and recovery.
 - South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall implement a policy to require personnel to report suspected information security incidents to the incident response team and/or South Carolina Workers' Compensation Commission leadership.

Information System Monitoring (SI 4)

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

Incident Response Training (IR 2)

- South Carolina Workers' Compensation Commission shall provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission shall establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.
 - South Carolina Workers' Compensation Commission shall
-

document the incident response test results and update incident response processes as applicable.

Malicious Code Protection (SI 3)

- South Carolina Workers' Compensation Commission shall employ malicious code protection mechanisms at information system entry and exit points to detect and eradicate malicious code.
- South Carolina Workers' Compensation Commission shall implement a process to help ensure malicious code protection mechanisms are updated whenever new releases are available.
- South Carolina Workers' Compensation Commission shall configure malicious code protection mechanisms to perform periodic scans at defined time intervals.
- South Carolina Workers' Compensation Commission 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) <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall develop and implement a process to identify, report, and correct information system flaws.• South Carolina Workers' Compensation Commission 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.• South Carolina Workers' Compensation Commission shall install latest stable versions of applicable security software and firmware updates.• South Carolina Workers' Compensation Commission shall establish a patch cycle that guides the normal application of patches and updates to systems.• South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission's information resources. The designation of an South Carolina Workers' Compensation Commission information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the South Carolina Workers' Compensation Commission'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 South Carolina Workers' Compensation Commission. If the South Carolina Workers' Compensation Commission does not designate an IRM, the title defaults to the South Carolina Workers' Compensation Commission'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.

South Carolina Workers' Compensation Commission

Information Security Policy – Access Control

V1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Access Control</i>	5
1.1 <i>Access Management</i>	5
1.2 <i>Network Access Management</i>	9
1.3 <i>Identity Management</i>	11
1.4 <i>Authentication</i>	12
1.5 <i>Emergency Access</i>	13
1.6 <i>Password Policy</i>	14
1.7 <i>Password Administration</i>	16
DEFINITIONS	17

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 South Carolina Workers’ Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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 South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

Account Management (AC 2)

- South Carolina Workers' Compensation Commission shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.
- South Carolina Workers' Compensation Commission shall identify authorized users of information system and specify access rights.
- South Carolina Workers' Compensation Commission shall establish a process to enforce access requests to be approved by business/data owner (or delegate) prior to provisioning user accounts.
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission established approval process.
- South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall review information system accounts within every one-hundred eighty (180) days and require annual certification.
- South Carolina Workers' Compensation Commission shall regulate information system access and define security requirements for contractors, vendors, and other service providers.
- South Carolina Workers' Compensation Commission shall establish procedures to administer privileged user accounts in accordance with a role-based access model.

Access Enforcement (AC 3)

- South Carolina Workers' Compensation Commission shall enforce approved authorizations for logical access to information systems.
- South Carolina Workers' Compensation Commission shall implement encryption as an access control mechanism if required by Federal, State or other laws or regulations.

Information Flow Enforcement (AC 4)

- For Restricted data: South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall document and implement separation of duties through assigned information system access authorizations.

Least Privilege (AC 6)

- South Carolina Workers' Compensation Commission shall ensure that only authorized individuals have access to South Carolina Workers' Compensation Commission 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".
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall automatically lock user accounts the after maximum logon attempts is reached. South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission systems shall

display the following warning before granting system access. “This system is solely for the use of authorized South Carolina Workers’ Compensation Commission personnel. The information contained herein is the property of South Carolina Workers’ Compensation Commission and subject to non-disclosure, security and confidentiality requirements. South Carolina Workers’ Compensation Commission shall monitor system usage for unauthorized activities. Any user accessing this system expressly consents to such monitoring.

- South Carolina Workers’ Compensation Commission implements warning banners that comply with Federal, State or other laws of regulations associated with the type of data handled by the South Carolina Workers’ Compensation Commission (e.g., For FTI IRS Publication 1075 requirements apply).

Session Lock (AC 11)

- South Carolina Workers’ Compensation Commission 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 South Carolina Workers' Compensation Commission information.
Policy	<p>Remote Access (AC 17)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall document allowed methods for remote access to the network and information systems.• South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission networks and information systems.• Remote users shall connect to South Carolina Workers' Compensation Commission information systems only using mechanism protocols approved by the South Carolina Workers' Compensation Commission through a limited number of managed access control points for remote connections.• For Restricted data and/or system administrators: South Carolina Workers' Compensation Commission employees and authorized third parties accessing South Carolina Workers' Compensation Commission information systems remotely shall do so via an approved two-factor authentication (2FA) technology.• South Carolina Workers' Compensation Commission 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). <p>Wireless Access (AC 18)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.• South Carolina Workers' Compensation Commission shall only use wireless networking technology that enforces user authentication.• South Carolina Workers' Compensation Commission shall authorize wireless access to information systems prior to allowing use of wireless networks.• South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission networks where information deemed critical by South Carolina Workers' Compensation Commission is stored or processed shall be physically or logically segregated from publicly available networks.
- South Carolina Workers' Compensation Commission networks and information systems shall not be accessible from public networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices.
- South Carolina Workers' Compensation Commission 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	<p>Identification and Authentication (IA 2, IA 4 AND IA 8)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission 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. • South Carolina Workers' Compensation Commission shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier. • South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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). • South Carolina Workers' Compensation Commission shall minimize the use of system, application, or service accounts; and South Carolina Workers' Compensation Commission shall document, formally approve, and designate a responsible party of this type of accounts. • South Carolina Workers' Compensation Commission 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	<p>NIST SP 800-53 Revision 4: IA 2 Identification and Authentication (Organizational Users)</p> <p>NIST SP 800-53 Revision 4: IA 4 Identifier Management</p> <p>NIST SP 800-53 Revision 4: IA 8 Identification and Authentication (Non-Organizational Users)</p>
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 South Carolina Workers' Compensation Commission for authenticating, external / remote access connections, VPN access, administrative function access, vendor access and remote access to sensitive information.
Policy	<p>Authenticator Management (IA 5)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user. <p>Unsuccessful Logon Attempts (AC 7)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall implement mechanisms to record successful and failed authentication attempts. <p>Session Lock (AC 11)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems. South Carolina Workers' Compensation Commission 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	<p>NIST SP 800-53 Revision 4: AC 7 Unsuccessful Logon Attempts</p> <p>NIST SP 800-53 Revision 4: AC 11 Session Lock</p> <p>NIST SP 800-53 Revision 4: IA 5 Authenticator Management</p>
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) <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.• The emergency procedures shall ensure that:<ul style="list-style-type: none">○ 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.• South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.
 - South Carolina Workers' Compensation Commission 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.
 - South Carolina Workers' Compensation Commission 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.).
-

-
- South Carolina Workers’ Compensation Commission shall suspend user accounts after a specified number of days of inactivity.
 - South Carolina Workers’ Compensation Commission 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	<p>Access Agreements (PS 6)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission users shall sign an acknowledgement to evidence understanding of authentication policies, including the South Carolina Workers' Compensation Commission policy to keep passwords confidential and to keep group passwords solely within the members of the group. • South Carolina Workers' Compensation Commission shall require that employees sign acknowledgement prior to allowing access to network and information systems. <p>Identification and Authentication (IA 2, IA 6 and IA 8)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall establish a process to verify the identity of a user prior to providing a new, replacement or temporary password. • South Carolina Workers' Compensation Commission shall establish a process to uniquely identify and authenticates non-Agency users. • South Carolina Workers' Compensation Commission shall establish procedures to manage new or removed privileged accounts passwords <p>Authenticator Management (IA 5)</p> <ul style="list-style-type: none"> • First-time passwords shall be set to a unique value per user and changed immediately after first use. • South Carolina Workers' Compensation Commission 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. • South Carolina Workers' Compensation Commission shall not allow default passwords for network and remote applications. <p>Authenticator Feedback (IA 6)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

South Carolina Workers' Compensation Commission

Information Security Policy – Data Protection and Privacy

v1.0 – October 10, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/10/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Data Protection and Privacy</i>	5
1.1 <i>Data Classification</i>	5
1.2 <i>Data Disposal</i>	7
1.3 <i>Data Protection</i>	8
1.4 <i>Privacy</i>	10
DEFINITIONS.....	12

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 are expected to comply with the State’s information security policies and may leverage them in revising existing or developing new policies. These policies exist in addition to all other South Carolina Workers’ Compensation Commission policies and federal and state regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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

Data Protection and Privacy

1.1 Data Classification

Purpose	The purpose of the data classification section is to define the different categories for South Carolina Workers' Compensation Commission information assets regardless of form whether it is electronic, hard copy, or intellectual property.
Policy	<p>Security Categorization (RA 2)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall categorize data in accordance with applicable federal and State laws, Executive Orders, directive, regulations, and information security guidance. South Carolina Workers' Compensation Commission data shall be classified into one of the following categories:<ol style="list-style-type: none">1. Public: Information intended or required for sharing publicly. Examples of public information include information provided on government website, and reports meant for public distribution. Unauthorized disclosure, alteration or destruction of Public data would result in minimum to no risk to the State.2. Internal Use: Information that is used in daily operations of the South Carolina Workers' Compensation Commission. Examples of internal use information include South Carolina Workers' Compensation Commission hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration or destruction of Internal Use data would result in little risk to the State.3. Confidential: Confidential information refers to sensitive information in custody of the South Carolina Workers' Compensation Commission. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration or destruction of confidential data would result in considerable risk to the State.4. Restricted: Restricted information is highly sensitive information in custody or owned by the South Carolina Workers' Compensation Commission and/or data which is protected by Federal or State laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration or destruction of Restricted data shall result in considerable risk to the State including

statutory penalties.

- Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or the South Carolina Workers' Compensation Commission Information Security and/or Data Privacy team(s) to determine the appropriate data classification.
- If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.

Policy Supplement	Refer to the <i>Division of Information Security</i> website for available enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: RA 2 Security Categorization
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Data Disposal

Purpose	The purpose of the data disposal section is to define the controls that shall be followed for disposal of data both in digital and non-digital formats.
Policy	<p>Media Sanitization (MP 6)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse and release outside of the South Carolina Workers' Compensation Commission based on applicable regulatory requirements.• South Carolina Workers' Compensation Commission shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.• South Carolina Workers' Compensation Commission shall establish controls mechanism and processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.• South Carolina Workers' Compensation Commission shall implement controls to track media sanitization and disposal process, wherein such actions shall be tracked, documented, and verified.• Media sanitization documentation shall provide a record of the media sanitized, when, how media was sanitized, the person who performed the sanitization, and the final disposition of the media. The record of action taken shall be maintained in a written or electronic format.• South Carolina Workers' Compensation Commission shall test media sanitization equipment and procedures at least annually to ensure correct performance.• FTI Receiving Agency only: South Carolina Workers' Compensation Commission sanitizing electronic media containing Federal Tax Information shall not make it available for reuse by other offices or released for destruction without first being subject to electromagnetic erasing.• South Carolina Workers' Compensation Commission shall define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be redeployed outside of the South Carolina Workers' Compensation Commission.• Approved processes like physical destruction or digital degaussing shall be performed on devices, before they are disposed.• South Carolina Workers' Compensation Commission shall destroy hard copy media containing internal-use, confidential or restricted information using approved methods prior to disposal.• The South Carolina Workers' Compensation Commission information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.

Policy Supplement	A policy supplement has not been identified.
Guidance	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 Data Protection

Purpose	The purpose of the encryption section is to define the controls that need to be in-place to protect confidential and restricted data.
Policy	<p>System and Communications Protection Policy and Procedures (SC 1)</p> <ul style="list-style-type: none"> • South Carolina Workers’ Compensation Commission employees shall follow South Carolina Workers’ Compensation Commission’s acceptable use policies when transmitting data. <p>Cryptographic Key Establishment and Management (SC 12)</p> <ul style="list-style-type: none"> • South Carolina Workers’ Compensation Commission implemented mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users. • South Carolina Workers’ Compensation Commission shall implement mechanisms to ensure the confidentiality of private keys. • South Carolina Workers’ Compensation Commission shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization. • South Carolina Workers’ Compensation Commission shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service. <p>Cryptographic Protection (SC 17)</p> <ul style="list-style-type: none"> • For Restricted or data protected by Federal or State laws or regulations: South Carolina Workers’ Compensation Commission shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data. • South Carolina Workers’ Compensation Commission shall implement all encryption mechanisms to comply with this policy and support a minimum of, but not limited to the industry standard, AES 128-bit encryption. • South Carolina Workers’ Compensation Commission shall not use any proprietary encryption algorithms for any purpose, unless approved by South Carolina Workers’ Compensation Commission’s information security department. <p>Transmission Confidentiality and Integrity (SC 8 and SC 9)</p> <ul style="list-style-type: none"> • Confidential or restricted information transmitted as an email message shall be encrypted based on South Carolina Workers’

	<p>Compensation Commission encryption policy.</p> <ul style="list-style-type: none">• Any confidential or restricted information transmitted through a public network to and from vendors, customers, or entities doing business with South Carolina Workers' Compensation Commission shall be encrypted or be transmitted through a tunnel encrypted by approved technologies such as virtual private networks (VPN), point-to-point tunnel protocols (PPTP) like secure socket layers (SSL).• South Carolina Workers' Compensation Commission shall implement wireless encryption standards such as Wi-Fi Protected Access 2 (WPA2), and VPN encryption for remote wireless and/or internal network configurations to encrypt wireless transmissions that are used for transmitting confidential or restricted information.• South Carolina Workers' Compensation Commission shall utilize encrypted file transfer programs such as "secured File Transfer Protocol (SFTP)" (FTP over Secure Shell (SSH) and Secure Copy (SCP) to secure transfer of documents and data over the Internet. Only authorized users shall be able to initiate secure transactions.
Policy Supplement	Refer to the Division of Information Security website for recommended enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: SC 1 System and Communications Protection Policy and Procedures NIST SP 800-53 Revision 4: SC 8 Transmission Integrity NIST SP 800-53 Revision 9: SC 8 Transmission Confidentiality NIST SP 800-53 Revision 4: SC 12 Cryptographic Key Establishment and Management NIST SP 800-53 Revision 4: SC17 Cryptographic Protection
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Privacy

Purpose	<p>The purpose of the privacy section is to set forth policies South Carolina Workers' Compensation Commission shall use when information systems or applications will gather Personal Identifiable Information (PII) and/or when webpages are available openly to the public.</p>
Policy	<p>Privacy Impact Assessment</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall conduct a Privacy Impact Assessment (PIA) on information systems that will handle Personal Identifiable Information (PII). • South Carolina Workers' Compensation Commission shall publish privacy policies on South Carolina Workers' Compensation Commission websites used by the public. • South Carolina Workers' Compensation Commission shall update PIAs when a system change creates new privacy risks (e.g., when functions applied to existing information collection change anonymous information into information in identifiable form). • PIAs shall include: <ol style="list-style-type: none"> a. What information is to be collected (e.g., nature and source); b. Why information is being collected (e.g., to determine eligibility) c. Intended use of information (e.g., to verify existing data); d. With whom the information will be shared; e. What opportunities individuals have to decline to provide information; f. How the information will be secured; • The PIA document shall be reviewed by an South Carolina Workers' Compensation Commission executive or designee, such as CIO, CISO, or similar. • Each South Carolina Workers' Compensation Commission is to provide a confidentiality agreement defining the responsibilities of the South Carolina Workers' Compensation Commission's employees and business partners (e.g., contractors, vendors) in maintaining the privacy of electronic information. • The South Carolina Workers' Compensation Commission electronic information privacy officer, in conjunction with the South Carolina Workers' Compensation Commission human resources department, is responsible for the development and administration of this confidentiality agreement. F T
Policy Supplement	<p>A policy supplement has not been identified.</p>
Guidance	<p>Fair Information Practice Principles (FIPPs)</p>

OMB Memorandum 03-22

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: 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 South Carolina Workers' Compensation Commission's information resources. The designation of an South Carolina Workers' Compensation Commission information resources manager is intended to establish clear accountability for setting policy for information resources management activities, provide for greater coordination of the South Carolina Workers' Compensation Commission'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 South Carolina Workers' Compensation Commission. If the South Carolina Workers' Compensation Commission does not designate an IRM, the title defaults to the South Carolina Workers' Compensation Commission'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.

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.

South Carolina Workers' Compensation Commission

Information Security Policy – Information Systems Acquisitions, Development, and Maintenance

v1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Information Systems Acquisitions, Development, and Maintenance</i>	<i>5</i>
1.1 Change Management	5
1.2 Configuration Management	6
1.3 System Development and Maintenance	7
1.4 Release Management	9
DEFINITIONS	11

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 South Carolina Workers' Compensation Commission policies and federal and state regulations governing the protection of South Carolina Workers' Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers' Compensation Commission 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 are associated 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.
- **Solution Reference:** Provides a uniform resource locator (URL) reference to the Recommended Technology Solutions.
- **Guidance:** Provides references to guidelines on information security policies.
- **Reference:** Provides a uniform resource locator (URL) reference to the guidance.

INFORMATION SECURITY POLICY

Information Systems Acquisitions, Development, and Maintenance

1.1 Change Management

Purpose	The purpose of the change management section is to ensure all changes are assessed, approved, implemented and reviewed in a controlled manner to production, and applicable non-production environments with minimal impact and risk.
<ul style="list-style-type: none">Policy	<p>Configuration Change Control (CM 3)</p> <ul style="list-style-type: none">South Carolina Workers' Compensation Commission shall define change management controls to manage changes to information systems in order to minimize the likelihood of disruption, unauthorized alterations and errors. The implementation of changes shall be controlled through the use of a change control process. The following recommendations shall be followed for the change control process:<ul style="list-style-type: none">All requests for change shall be handled in a structured way that determines the impact on the operational system and its functionality;All changes to production environments, including emergency maintenance and patches, shall be formally managed in a controlled manner.South Carolina Workers' Compensation Commission shall have a process to categorize, prioritize and authorize changes to information systems;Post-implementation reviews shall be performed to ensure production changes are operating as intended;A process shall be defined and communicated to ensure that all new modifications to the production environment have been adequately tested;A process for defining, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process shall be established; andInformation systems shall be reviewed and tested after major changes to operating systems.
Policy Supplement	A policy supplement has not been identified.
Solution Reference	An enterprise solution has currently not been identified for this section.
Guidance	NIST SP 800-53 Revision 4: CM 3 Configuration Change Control
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.2 Configuration Management

Purpose	<p>The purpose of the configuration management section is to establish procedures for the compliance with minimally acceptable system configuration requirements, as determined by [Agency]. In addition, this section helps ensure South Carolina Workers' Compensation Commission establish processes to identify and implement secure configurations, control configuration changes, and monitor security controls to validate adherence with approved configurations.</p>
Policy	<p>Baseline Configuration (CM 2)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall develop, review, and formally approve baseline configurations (most secure state) for critical information systems and infrastructure components.• South Carolina Workers' Compensation Commission shall develop a process to manage changes to baseline configurations, including identification, review, security impact analysis, test, and approval prior to implementation of changes.• South Carolina Workers' Compensation Commission shall establish a central repository of all baseline configurations and shall implement access restrictions to prevent unauthorized changes.• South Carolina Workers' Compensation Commission shall retain older versions of baseline configurations to be able to support rollback.• South Carolina Workers' Compensation Commission shall review and update baseline configurations periodically, and/or as an integral part of information system component installations or upgrades. <p>Configuration Management Plan (CM 9)</p> <ul style="list-style-type: none">• The South Carolina Workers' Compensation Commission shall assign responsibilities for developing and managing the configuration management process to personnel that are not directly involved in system development activities.
Policy Supplement	<p>A policy supplement has not been identified.</p>
Solution Reference	<p>An enterprise solution has currently not been identified for this section.</p>
Guidance	<p>NIST SP 800-53 Revision 4: CM 2 Baseline Configuration NIST SP 800-53 Revision 4: CM 9 Configuration Management Plan NIST SP 800-128: Guide for Security-Focused Configuration Management of Information Systems</p>
Reference	<p>http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</p>

1.3 System Development and Maintenance

Purpose

The purpose of the system development and maintenance section is to define requirements for system security planning and to improve protection of South Carolina Workers' Compensation Commission information system resources.

Policy

System Security Plan (PL 2)

- South Carolina Workers' Compensation Commission shall prepare system security plans and documentation for critical enterprise information systems or systems under development.
- System security plans shall provide an overview of the security requirements of the system and describe the controls in place for meeting the requirements through all stages of the systems development life cycle.
- When the system is modified in a manner that affects security, system documentation shall be updated accordingly.

Vulnerability Scanning (RA 5)

- South Carolina Workers' Compensation Commission shall perform a vulnerability assessment on all enterprise information systems undergoing significant changes, before the systems are moved into production.
- South Carolina Workers' Compensation Commission shall perform periodic vulnerability assessments on production enterprise information systems and take appropriate measures to address the risks associated with any identified vulnerabilities.
- Vulnerability notifications from vendors and other appropriate sources shall be monitored and assessed for all information systems and applications.

System and Services Acquisition Policy and Procedures (SA 2)

- South Carolina Workers' Compensation Commission shall develop and follow a set of procedures consistent with State procurement standards as defined by the Division of Information Security and the Information Technology Management Office.
- South Carolina Workers' Compensation Commission shall ensure that the State's interests have been protected and enforced in all IT procurement contracts.

System Development Life Cycle (SA 3)

- South Carolina Workers' Compensation Commission shall implement appropriate security controls at all stages of the information system life cycle

External Information System Services (SA 9)

- South Carolina Workers' Compensation Commission shall supervise and monitor outsourced software development to validate South Carolina Workers' Compensation Commission security requirements.

Developer Security Testing and Evaluation (SA-11)

- South Carolina Workers' Compensation Commission shall establish
-

separate development, testing, and production environments

- South Carolina Workers' Compensation Commission shall not use production data for testing purposes unless the data has been obfuscated, sanitized, or declassified. If production data must be temporarily used in these environments, appropriate security controls, including management approval, procedures to remove/delete data after completion of tests, and documentation of activities, shall be implemented.

Flaw Remediation (SI 2)

- South Carolina Workers' Compensation Commission shall design appropriate controls into information systems, including user developed applications to ensure correct processing.
- South Carolina Workers' Compensation Commission shall ensure that software patches are applied when they function to remove or reduce security weaknesses.

Security Alerts, Advisories, and Directives (SI 5)

- South Carolina Workers' Compensation Commission shall establish a process to collect information system security alerts, advisories, and directives on patches on an ongoing basis and implement these security directives in accordance with established time frames.
- A specific group or individual shall be given responsibility for monitoring vulnerabilities and vendors' releases of patches and fixes.

Software, Firmware, and Information Integrity (SI 7)

- South Carolina Workers' Compensation Commission shall ensure that any decision to upgrade to a new release shall take into account the business requirements for the change, and the security of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).
- South Carolina Workers' Compensation Commission shall test critical operating system (OS) changes and updates in the test environment to ensure there is no adverse impact on organizational operations or security.

Information Input Validation (SI 10)

- South Carolina Workers' Compensation Commission shall incorporate controls into information systems to check the validity of information inputs and information outputs.
- South Carolina Workers' Compensation Commission shall incorporate processing validation checks into information systems to detect processing errors, inadvertent or deliberate processing actions (e.g., accidental deletions).

Session Authenticity (SC 23)

- South Carolina Workers' Compensation Commission shall identify the appropriate controls to ensure session authenticity, protecting message integrity in applications and protecting information transmission to and from information systems.

	Threat and Vulnerability Management 1.2: Vulnerability Assessment Solution
Solution Reference	Refer to the Division of Information Security website for available enterprise solutions.
Guidance	NIST SP 800-53 Revision 4: PL 2 System Security Plan NIST SP 800-53 Revision 4: RA 5 Vulnerability Scanning NIST SP 800-53 Revision 4: SA 2 System and Services Acquisition Policy and Procedure NIST SP 800-53 Revision 4: SA 3 System Development Life Cycle NIST SP 800-53 Revision 4: SA 9 External Information System Services NIST SP 800-53 Revision 4: SA 11 Developer Security Testing and Evaluation NIST SP 800-53 Revision 4: SI 2 Flaw Remediation NIST SP 800-53 Revision 4: SI 7 Software, Firmware, and Information Integrity NIST SP 800-53 Revision 4: SI 10 Information Input Validation NIST SP 800-53 Revision 4: SC 23 Session Authenticity
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.4 Release Management

Purpose	The purpose of the release management section is to define the appropriate release activities during an implementation or upgrade of information systems.
---------	---

Policy

Allocation of Resources (SA 2)

- South Carolina Workers' Compensation Commission shall ensure that production-ready release packages have been deployed using the release management lifecycle (i.e., plan, prepare, build and test, pilot, and deploy).
- South Carolina Workers' Compensation Commission shall determine as part of the release planning process:
 - Resources required to deploy the release;
 - Pass/fail criteria;
 - Build and test plans prior to implementation;
 - Pilot and deployment plans; and
 - Develop requirements for the release.

Information System Documentation (SA 5)

- South Carolina Workers' Compensation Commission shall document the set of tools and processes used to manage the IT release lifecycle, and the prioritization of the release;
- South Carolina Workers' Compensation Commission shall validate the release design against the requirements, and identify the risks and potential issues.

Security Engineering Principles (SA 8)

- South Carolina Workers' Compensation Commission shall implement standardization and enforce operational controls through the use of change requests for deploying releases into production.

Policy Supplement

A policy supplement has not been identified.

Solution Reference

An enterprise solution has currently not been identified for this section.

Guidance

NIST SP 800-53 Revision 4: SA 2 Allocation of Resources
NIST SP 800-53 Revision 4: SA 5 Information System Documentation
NIST SP 800-53 Revision 4: SA 8 Security Engineering Principles

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 valid credential.

Authorization: Authorization is the process of enforcing policies, and 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 alphanumeric passwords.

Cryptography: A method of converting clear text into undecipherable text and later reversing the process to create readable text.

Data at rest: All data in storage, regardless of the storage device. 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.

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, tablets, mobile computers, 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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

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 Agency'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 Agency. 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 Agency, roles are relatively stable, while users and permissions are both numerous and may change rapidly.

Segregation of Duties: The separation of duties to prevent conflicts of interest and ensure that no changes are executed without being observed by another individual. The purpose of the control is to minimize fraud, error, and omission.

System development life cycle (SDLC): A multistep process to develop or acquire systems that starts with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

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. Two-factor authentication refers to the use of two of these three factors listed above.

South Carolina Workers' Compensation Commission

Information Security Policy – Mobile Security

v1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Mobile Security</i>	5
1.1 <i>Mobile Security</i>	5
1.2 <i>Removable Media Security</i>	8
1.3 <i>Portable Computing Devices</i>	9
DEFINITIONS.....	10

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 South Carolina Workers' Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers' Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers' Compensation Commission 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	<p>State business requirements may, on occasion, justify storing confidential data on mobile computing devices. It is the responsibility of the South Carolina Workers' Compensation Commission to recognize the associated risks and take the necessary steps to protect and secure their mobile computing devices.</p> <p>Device Identification (MP 7)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission only allows portable media devices when these are assigned and identified to an individual owner.• South Carolina Workers' Compensation Commission only allows the use of portable media devices that allow sanitization.• South Carolina Workers' Compensation Commission shall use mobile devices that have the ability to be remotely wiped / erased. <p>Access Control for Mobile Devices (AC 19)</p> <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall develop usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.• South Carolina Workers' Compensation Commission shall develop a list of approved mobile devices. Only approved mobile devices shall be allowed to access the [Agency]'s network and information systems.• South Carolina Workers' Compensation Commission shall develop and apply adequate asset management procedures to all mobile devices.• South Carolina Workers' Compensation Commission shall utilize the approved encryption standard for mobile devices.• South Carolina Workers' Compensation Commission shall implement controls to centrally manage the installation of standardized operating system, applications and patches on mobile devices.• South Carolina Workers' Compensation Commission shall remove sensitive and confidential information from the mobile device before it is disposed.• South Carolina Workers' Compensation Commission 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, South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission shall disable all mobile device options and applications that are not in use or required by users' duties.
- South Carolina Workers' Compensation Commission shall protect all mobile devices with password or Personal Identification Number (PIN).
- South Carolina Workers' Compensation Commission shall ensure all mobile devices have timeout/locking features.
- South Carolina Workers' Compensation Commission shall develop controls for the protection of data storage on mobile devices including removable media.
- South Carolina Workers' Compensation Commission 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.
- South Carolina Workers' Compensation Commission 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)

- South Carolina Workers' Compensation Commission 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	<p>Media Protection Policy and Procedures (MP 1)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures. <p>Media Storage (MP 4)</p> <ul style="list-style-type: none"> For sensitive data, South Carolina Workers' Compensation Commission shall physically control and securely store digital (e.g., CD, flash drives) and non-digital (e.g., paper) media within secured locations. South Carolina Workers' Compensation Commission shall ensure that only secure portable storage devices (e.g., encrypted flash drives) are utilized as removable media. <p>Media Transport (MP 5)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission shall employ encryption mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas. South Carolina Workers' Compensation Commission shall establish a process to enforce accountability for removable media during transport outside of controlled areas. <p>Media Sanitization (MP 6)</p> <ul style="list-style-type: none"> South Carolina Workers' Compensation Commission 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	<p>NIST SP 800-53 Revision 4: MP 1 Media Protection Policy and Procedures</p> <p>NIST SP 800-53 Revision 4: MP 4 Media Storage</p> <p>NIST SP 800-53 Revision 4: MP 5 Media Transport</p> <p>NIST SP 800-53 Revision 4: MP 6 Media Sanitization</p>
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	<p>Access Control for Mobile Devices (AC 19)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall employ whole disk encryption to protect the confidentiality and integrity of information stored on computing devices, including laptops. • South Carolina Workers' Compensation Commission shall configure computing devices operating system (OS) so that only approved services are enabled and/or installed. • South Carolina Workers' Compensation Commission 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. • South Carolina Workers' Compensation Commission shall implement tools to automatically update virus definition files on laptops and other portable computing devices susceptible to viruses. • South Carolina Workers' Compensation Commission 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. • South Carolina Workers' Compensation Commission shall place asset tags on portable computing devices. • South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

South Carolina Workers' Compensation Commission

Information Security Policy – Risk Management

v1.0 – October 17, 2014

Revision History

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

Date	Authored by	Title	Ver.	Notes
10/17/2014	Betsy Hartman	IT Director	1.0	Based on DIS final policy

Table of Contents

INTRODUCTION	3
PART 1. PREFACE	3
PART 2. ORGANIZATIONAL AND FUNCTIONAL RESPONSIBILITIES	3
PART 3. PURPOSE.....	4
PART 4. SECTION OVERVIEW	4
INFORMATION SECURITY POLICY	5
<i>Risk Management.....</i>	<i>5</i>
1.1 <i>Risk Management.....</i>	<i>5</i>
1.2 <i>Risk Assessment.....</i>	<i>6</i>
1.3 <i>Risk Mitigation.....</i>	<i>8</i>
DEFINITIONS.....	9

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 South Carolina Workers’ Compensation Commission policies and federal and State regulations governing the protection of South Carolina Workers’ Compensation Commission data. Adherence to the policies will improve the security posture of the State and help safeguard South Carolina Workers’ Compensation Commission 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.
- **Solution Reference:** Provides a reference to the Recommended Technology Solutions in the form of a uniform resource locator (URL).
- **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

Risk Management

1.1 Risk Management

Purpose	<p>The purpose of the risk management section is to define the controls that shall be implemented by South Carolina Workers' Compensation Commission to identify and assess information security risks, and to take steps to reduce risk to an acceptable level.</p> <p>Risk management typically consists of the following:</p> <ul style="list-style-type: none"> • Risk Assessment: A risk assessment is the first process of risk management, and is used to determine the extent of the potential threat and the risk associated with IT security. • Risk Mitigation: Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls for the risks identified during the risk assessment process.
Policy	<p>Risk Management Strategy (PM 9)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall define a schedule for an on-going risk assessment and risk mitigation process. • South Carolina Workers' Compensation Commission shall review and evaluate risk based on the system categorization level and/or data classification of their systems.
Policy Supplement	<p>A risk self-assessment tool has been created by the Division of Information Security. This tool can be leveraged by Agencies/Institutions to perform a risk assessment based on a risk framework developed for the State. See self-assessment tool at https://www.bcbis.sc.gov/DIS/DIS-index.phtm</p>
Solution Reference	<p>An enterprise solution has currently not been identified for this section.</p>
Guidance	<p>NIST SP 800-53 Revision 4: PM 9 Risk Management Strategy</p>
Reference	<p>http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx</p>

1.2 Risk Assessment

Purpose	The purpose of the risk assessment section is to define a process to identify and manage IT security risks and ensure ongoing compliance with applicable State laws and regulations.
Policy	<p>Risk Assessment (RA 3)</p> <ul style="list-style-type: none"> • The South Carolina Workers' Compensation Commission shall establish a risk assessment framework based on applicable State and federal laws, regulation, and industry standards (e.g., NIST 800-30). This assessment framework shall clearly define accountability, roles and responsibilities. <p>Security Assessment (CA 2)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall annually conduct a formal assessment of the IT security processes and controls to determine the appropriateness of the design and implementation of controls, and the extent to which the controls are operating as intended and producing the desired outcome with respect to meeting the security requirements for their systems (e.g., NIST SP 800-115). • South Carolina Workers' Compensation Commission shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the [Agency]. <p>Plan of Action and Milestones (CA 5)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall develop and periodically update a Plan of Action & Milestones (POAM) document that shall identify any deficiencies related to internal security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments. • South Carolina Workers' Compensation Commission shall develop and periodically update a Corrective Action Plan (CAP) to identify activities planned or completed to correct deficiencies identified during the security assessment review. Both the POAM and the CAP shall address implementation of security controls to reduce or eliminate known risks in South Carolina Workers' Compensation Commission systems. <p>Security Authorization (CA 6)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall establish a process and assign a senior-level executive or manager to determine whether or not risks can be accepted, and for each of the risks identified following the risk assessment, the designated personnel within the South Carolina Workers' Compensation Commission shall make a decision regarding risk treatment. <p>Continuous Monitoring (CA 7)</p> <ul style="list-style-type: none"> • South Carolina Workers' Compensation Commission shall continuously monitor the security controls within its information

	systems to ensure that the controls are operating as intended.
Policy Supplement	A policy supplement has not been identified.
Solution Reference	An enterprise solution has currently not been identified for this section.
Guidance	NIST SP 800-15 NIST SP 800-53 Revision 4: RA 3 Risk Assessment NIST SP 800-53 Revision 4: CA 2 Security Assessment NIST SP 800-53 Revision 4: CA 5 Plan of Action and Milestones NIST SP 800-53 Revision 4: CA 6 Security Authorization NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring
Reference	http://csrc.nist.gov/publications/nistpubs/800-53-rev4/sp800_53_r4_final_word_ver.docx

1.3 Risk Mitigation

Purpose	The purpose of the risk mitigation section is to support mitigation of risks identified and to define the level of risk that is acceptance to the South Carolina Workers' Compensation Commission where risks are accepted knowingly and objectively.
Policy	Continuous Monitoring (CA 7) <ul style="list-style-type: none">• South Carolina Workers' Compensation Commission shall establish and implement controls to ensure risks are reduced to an acceptable level based on security requirements and once threats have been identified and decisions for the management of risks have been made.• South Carolina Workers' Compensation Commission shall determine and document the acceptable level for risk for various threats based on the business requirements and the impact of the potential risk to the [Agency].
Policy Supplement	A policy supplement has not been identified.
Solution Reference	An enterprise solution has currently not been identified for this section.
Guidance	NIST SP 800-53 Revision 4: CA 7 Continuous Monitoring
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 valid credential.

Authorization: Authorization is the process of enforcing policies, and 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 alphanumeric passwords.

Cryptography: A method of converting clear text into undecipherable text and later reversing the process to create readable text.

Data at rest: All data in storage, regardless of the storage device. 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.

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, tablets, mobile computers, 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 South Carolina Workers' Compensation Commission 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 South Carolina Workers' Compensation Commission 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.

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 Agency'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 Agency. 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 Agency, roles are relatively stable, while users and permissions are both numerous and may change rapidly.

Segregation of Duties: The separation of duties to prevent conflicts of interest and ensure that no changes are executed without being observed by another individual. The purpose of the control is to minimize fraud, error, and omission.

System development life cycle (SDLC): A multistep process to develop or acquire systems that starts with initiation, analysis, design, and implementation, and continues through the maintenance and disposal of the system.

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. Two-factor authentication refers to the use of two of these three factors listed above.