State of South Carolina – Division of Information Security (DIS)

# Information Security Policy Handbook

# Document Change History

| Version Number | Release Date | Summary of Changes | Section No./ Paragraph No. | Changes Made By |
|---|---|---|---|---|
| 1.0 | 22-Oct-2014 | Initial release | | |
| 1.1 | 03-Nov-2014 | Corrected Table 2 “Deadlines for Policy Implementation” – removed upload requirements. | sect 1.3 | David Wilhite |
| | | | | |
| | | | | |

# Table of Contents

**1. Purpose and Scope ..... 4**

1.1. Purpose ..... 4

1.2. Statewide Information Security Policies ..... 4

1.3. Information Security Policy Overview ..... 5

1.4. Policy Adoption Preparation ..... 6

**2. Information Security Policy Deployment ..... 8**

2.1. Approach ..... 8

Step 1 – InfoSec Policies Analysis ..... 8

Step 2 – InfoSec Executive Management Approval & Policies Implementation ..... 17

Step 3 – InfoSec Policies Awareness ..... 17

Additional Information ..... 19

# 1. Purpose and Scope

## 1.1. Purpose

The purpose of this handbook is to provide agencies detailed guidance on the policy implementation processes and tools provided by the Division of Information Security (DIS). Its use may vary by audience: 1) providing reference materials to agencies that participated in the policy training workshops, onsite visits, and pilots, or 2) providing detailed guidance and instruction to agencies that did not participate in the activities listed above. The handbook is structured as follows:

- Policy Implementation Approach / “How To” – Guidance on completion of the supporting documents and templates. This also presents recommendations for solutions to common challenges agencies face as they complete the implementation process.
- Lessons Learned – Additional guidance on the interpretation and adoption of 10 core policies based upon feedback obtained through the workshops, onsite visits, and pilots.
- Sample Templates – A sample completed Roles and Responsibilities Chart, a completed Gap Analysis template, and completed Implementation Plan template for the Asset Management policy.

Using the information contained here, agencies should have the information needed to execute the policy implementation process. *For further details, refer to Appendix A.*

## 1.2. Statewide Information Security Policies

DIS has developed and published thirteen (13) statewide information security policies that set forth the minimum requirements agencies must implement to protect information assets from unauthorized disclosure, misuse, alteration, or destruction, in a manner that meets risk management expectations. Refer to “Table 1: Information Security Policies” below for a list of the statewide information security policies.

**Table 1. Information Security Policies**

| State of South Carolina Information Security Policies | |
|---|---|
| Master Policy | IT Risk Strategy Policy |
| Asset Management Policy | Mobile Security Policy |
| Data Protection and Privacy Policy | Human Resources and Security Awareness Policy |
| Access Control Policy | Physical Environmental Security Policy |
| Information Systems Acquisitions Development and Maintenance Policy | Risk Management Policy |
| Threat Vulnerability Management Policy | IT Compliance Policy |
| Business Continuity Management Policy | |

An effective information security plan improves the security posture and aligns information security with an agency's mission, goals, and objectives. The Information Security policies were finalized by DIS in April of 2014 and are posted on the DIS website (http://dis.sc.gov) under the *Policies and Procedures* tab. *For further details related to the policies, refer to Appendix B.*

## 1.3. Information Security Policy Overview

Policy implementation must include the following components:

1. ***Policy Adoption*** **–** Each agency must adopt statewide information security policies, by aligning its documented procedures and controls with the published statewide policies.
2. ***Executive Support*** **–** Agency executive management must approve of documented procedures and controls, and commit necessary resources to their implementation and enforcement.
3. ***Enabling Policies*** **–** Each agency must implement its documented procedures and controls, by training personnel with necessary skills, by adjusting business processes to provide appropriate security, and by implementing security technology where needed.
4. ***Policy Awareness*** **–** Each agency must promote awareness and adherence to procedures and controls among its employees and contractors.

Agencies are to reach full implementation by meeting the schedule shown in Table 2:

**Table 2. DIS Deadlines for Policy Implementation**

| State of South Carolina Information Security Policy Implementation Timeline | |
|---|---|
| Activity | Deadline |
| Document Roles & Responsibilities | June  30, 2014 |
| Document Implementation Plan(s) | January 31, 2015 |
| Policy Compliance Date | July 01, 2016 |

- ***June 30, 2014*** – ***Roles and Responsibilities*** – By this date, agencies were expected to have completed the 'Roles and Responsibilities Chart' (or equivalent template) posted on the DIS website. *For further details on the Roles and Responsibilities Chart template, please see section 2.2.*
- **January 31, 2015 – Implementation Plans** – Each agency must perform a gap analysis, between statewide policy and the agency's current documented practices, noting any deficiencies or missing controls. By this date, each agency must document a plan for remediating gaps. For further details on the Gap Analyses and Implementation Plan templates, please see section 2.2.
- ***July 1, 2016*** **–** ***Compliance Date*** – By this date, each agency must complete execution of its implementation plans.

For further details on each of the DIS deadlines, refer to Appendix B.

## 1.4. Policy Adoption Preparation

There are three strategy options recommended by DIS for documenting processes and controls to align with state policies, based on conversations with policy champions. As the policy champion, one should understand each of the strategies mentioned and adapt them in a manner that is best suited for the agency.

1. ***Policy Mapping*** – Using this strategy, an agency can map the missing pieces or gaps from the thirteen state policies into their existing policies or procedures and continue to utilize the existing policies and procedures (with additions as needed) for governance.
2. ***Adopt & Reference Policies and Align Procedures*** – In this strategy, similar to the 'policy mapping' method, the agency can plug in missing pieces from the thirteen state policies into their existing procedures, and reference the state policies from the internal procedures. You may continue to have existing policies in addition to referencing the state policies, but in this strategy, an agency acknowledges state policies, and modifies or creates new procedures as needed to comply with state policies.

3. ***Customization of State Policies*** – Using this strategy, an agency may download each of the thirteen state policies and review line by line, bullet by bullet, to tailor the policy to fit the agency.

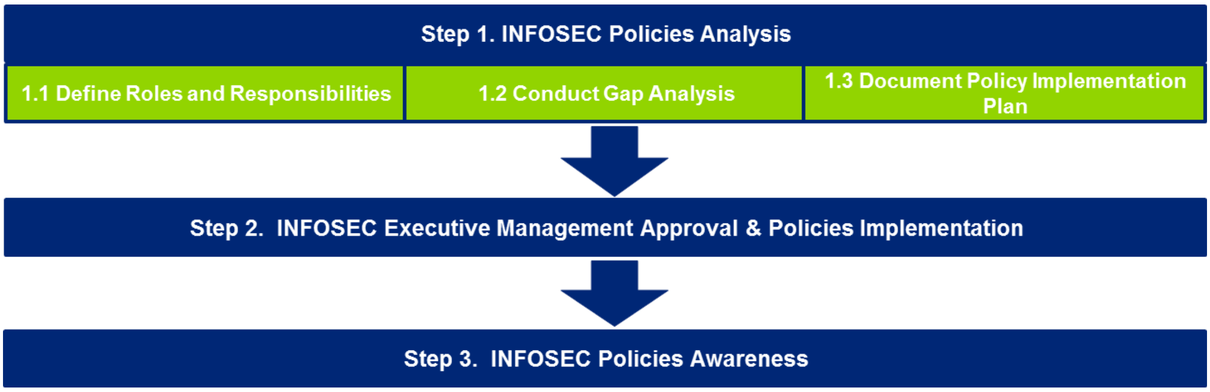
For further details and explanations on each of the strategies mentioned, refer to Appendix B.

# 2. Information Security Policy Deployment

## 2.1. Approach

The following diagram and detailed outline breaks down the approach an agency should take for implementing state policies. There are three major steps towards implementation, each detailed in the subsequent sections below. Step 1, InfoSec Policies Analysis, is an analysis of where the agency stands today against the state policies, and how the agency plans to address the gaps. Step 2, InfoSec Executive Management Approval & Policies Implementation, involves the review process associated with agency policies, approval from agency leadership, and implementation of agency policy to govern employees. Step 3, InfoSec Policies Awareness, guides readers through different training techniques that can be used for policy awareness for the approved and implemented policies.

Figure 1. Information Security Policy Deployment Approach


Step 1. INFOSEC Policies Analysis
1.1 Define Roles and Responsibilities
1.2 Conduct Gap Analysis
1.3 Document Policy Implementation Plan
Step 2. INFOSEC Executive Management Approval & Policies Implementation
Step 3. INFOSEC Policies Awareness

## 2.2. Step 1 – InfoSec Policies Analysis

For Step 1, InfoSec Policies Analysis, the process to analyze the agency's environment against the state policies is further broken into 3 sub-steps.

First, an agency should define their *Roles and Responsibilities*, meaning that they should identify the individuals who have the knowledge and skillsets for the processes identified in the policies, as well as those individuals who need to review and approve each policy.

The second sub-step involves *Gap Analyses,* as the agency identifies the areas where they are not compliant with the state policies.

Finally, based on the gaps identified, the agency should draft *Implementation Plans* to build out the remediation strategy that will be used to close the open gaps. The below sections provide further details on the background, approach and challenges associated with each sub-step of Step 1, InfoSec Policies Analysis.

### 2.2.1. Define Roles and Responsibilities

Assigning roles and responsibilities enables an agency to identify the various team members required to describe an agency's policy deployment initiative.  It is essential for agencies to identify the business teams (e.g., HR Team, IT Team, and Network Team) or individuals to complete assignments and deliverables for the adoption of each information security policy. The roles and responsibilities chart helps team leaders and agency members to understand their roles and responsibilities on the information security policies deployment effort. Role assignments should be transitory, meaning that they are not full time positions, and should be performed during the planning process of the information security policy deployment. Ideally, roles and responsibilities should be acknowledged and accepted with staff sharing the execution of multiple assignments.

The following sections outline the approach that an agency can follow to define main roles and responsibilities, challenges that an agency can face when establishing roles, responsibilities, and management commitment. A sample template that illustrates a completed sub-set of the Roles and Responsibilities Chart can be found in Appendix C - Sample Roles and Responsibility Chart in the Information Security Policy Handbook Appendices document.

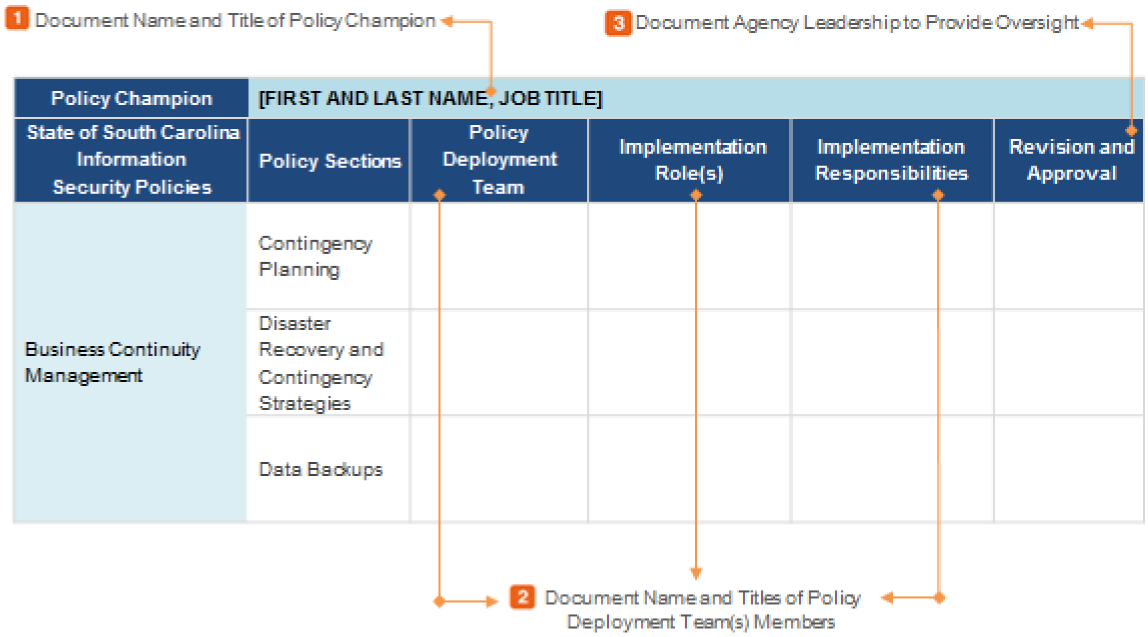
#### *Approach for Roles & Responsibilities Chart*

To define the roles and responsibilities that need to be involved during the information security policy deployment, an agency can use the "Roles and Responsibilities Chart" published on the DIS's website (http://dis.sc.gov/resources).  An agency may tailor this template as needed in order to make it appropriate to their environment.

Figure 2 below shows general guidelines on how to use the Roles and Responsibilities Chart to assign the main roles and responsibilities applicable to adopt the information security policies at agencies.

**Figure 2. Components of the Roles and Responsibilities Chart**

Roles and Responsibilities Chart - Template



1 Document Name and Title of Policy Champion

3 Document Agency Leadership to Provide Oversight

| Policy Champion | [FIRST AND LAST NAME, JOB TITLE] | | | | |
|---|---|---|---|---|---|
| State of South Carolina Information Security Policies | Policy Sections | Policy Deployment Team | Implementation Role(s) | Implementation Responsibilities | Revision and Approval |
| Business Continuity Management | Contingency Planning | | | | |
| | Disaster Recovery and Contingency Strategies | | | | |
| | Data Backups | | | | |

2 Document Name and Titles of Policy Deployment Team(s) Members

1 Document Name and Title of Policy Champion

A Policy Champion will be designated to lead the information security policies adoption effort for the agency. This individual should have a management or supervisory role within the agency in the areas of compliance, information security and/or information technology. The Policy Champion should serve as a liaison between agency leadership and the Policy Deployment Team(s). Depending on agency size, type of data handled, and organization structure, some agencies may require more than one Policy Champion.

An agency should document the full name (first and last name) and the job title (e.g., software developer, database administrator, etc.) of the Policy Champion on the Roles and Responsibilities Chart

2 Document Name and Titles of Policy Deployment Team(s) Members

In addition to Policy Champions, the agency should identify a Policy Deployment Team(s) for each information security policy. The Policy Deployment Team(s) should have pertinent knowledge of the policy topics they are being assigned for adoption. A Policy Deployment Team can be comprised of different departments or business roles (e.g., HR department, IT department, etc.). The agency should define the roles and responsibilities for each member of the Policy Deployment Team. Names (first and last name) and job titles (e.g., Software Developer, Database Administrator, etc.) should be documented on the Chart.

For the Policy Deployment Team column, the agency should fill in the names of employees, departments or organizations where applicable. For the Implementation Role(s) column, the agency should identify roles associated with each of the names or departments identified in the previous column. For the Implementation Responsibilities column, the agency should define the roles further and document associated responsibilities of those individuals or departments.

The main role of the Policy Deployment Team is to produce policies and/or procedures that will enable the agency to adopt and comply with the State's information security policies. Some sample roles and respective responsibilities of the Policy Deployment Team(s) are as follows:

- **Documentation Team/Lead:** Responsible for collecting the relevant documentation of existing policies, standards, and procedures with respect to the policy (or policy section) under review. Also, this individual/team is also responsible for supporting the documentation of the gap analysis and the policy implementation plan
- **Gap Analysis Team/Lead:** Responsible for reviewing existing policies, standards, and procedures and conducting the gap analysis for the policy under review. The individuals in this role should have pertinent knowledge to the specific policy section.
- **Implementation Plan Team/Lead:** Responsible for developing the policy implementation plans based on the particular gaps identified on the gap analysis. This individual/team is also responsible for identifying deployment challenges and risks.
- **Procedure Development Team/Lead:** Responsible for providing guidance for the implementation of processes to meet policy requirements, and for developing or updating the procedures based on the gap analysis and implementation plan.
- **Data Champion:** This individual is responsible for performing data classification according to the state data classification schema and completing the data inventory tool.

For some agencies it may not be possible to delegate tasks to multiple individuals. In this case, the Policy Champion may be responsible for the overall adoption of policies. And in general, a single individual may be assigned to two or more areas.

3 Document Agency Leadership to Provide Oversight

The agency should identify executive level personnel (i.e., Agency Director, IT Director, Information Security Liaison, etc.) responsible for overseeing the policy adoption efforts, including the review and approval of the Roles and Responsibilities Chart and other products related to the policy adoption initiative. The main responsibility of Agency Leadership is to support and provide guidance to the Policy Champion and Policy Implementation Team(s) to help build policy adoption plans that are sound, and implementation dates that are feasible.

Agency leadership members (full names and job titles) should be documented on the Roles and Responsibilities Chart

For further details and challenges associated with the Roles & Responsibilities Chart, refer to Appendix C.

### 2.2.2. Conduct Gap Analysis

After defining roles and responsibilities, the next step involves conducting gap analyses, evaluating the agency's current processes compared to state requirements defined in the statewide information security policies. The gap analysis step is one of the fundamental components that help develop, define and improve an agency's information security plan. It is essential for agencies to perform the gap analyses with the business teams (e.g., HR Team, IT Team, etc.), which should be identified in the Roles and Responsibilities Chart, and/or the main individuals involved with the specific domain, in order to better analyze the current state of the agency. The gap analyses phase is meant to be completed *once* (per policy) as a point in time exercise used to identify gaps for the foundation of the implementation plans (sub-step 1.3).

The following section outlines the approach that an agency can follow to perform gap analysis for each of the thirteen state policies. A sample template that illustrates a completed Gap Analysis for Asset Management can be found in Appendix D - Sample Gap Analysis – Asset Management in the Information Security Policy Handbook Appendices document.

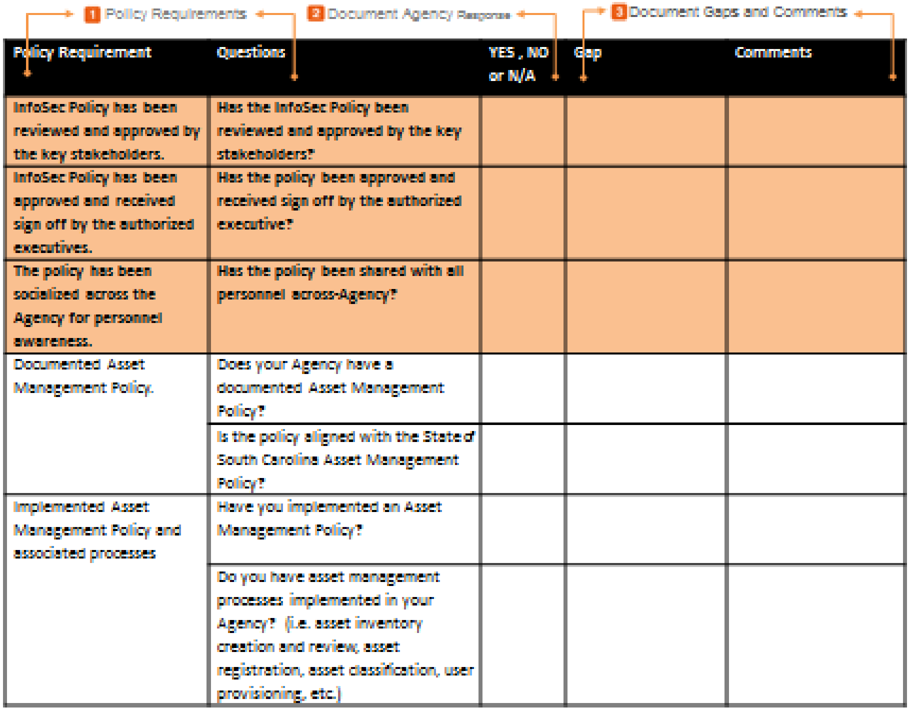
#### *Approach for Gap Analysis*

The different gap analysis templates for the thirteen statewide information security policies have been published to the DIS Website (http://dis.sc.gov/resources) under the resources tab. The gap analysis template contains a series of simplified questions that outline each bulleted requirement corresponding with that Information Security policy. Agencies should go through each gap analysis and document the response to the questions present in the template, including comments and detailed descriptions of identified gaps. An agency may tailor this template as needed in order to make it appropriate to the agency's environment and requirements.

Figure 3 below shows general guidelines on how to use the gap analysis template and how to perform various gap analyses.

### Figure 3. Components of the Gap Analysis Template

Gap Analysis - Template


1 Policy Requirements
2 Document Agency Response
3 Document Gaps and Comments

| Policy Requirement | Questions | YES , NO or N/A | Gap | Comments |
|---|---|---|---|---|
| InfoSec Policy has been reviewed and approved by the key stakeholders. | Has the InfoSec Policy been reviewed and approved by the key stakeholders? | | | |
| InfoSec Policy has been approved and received sign off by the authorized executives. | Has the policy been approved and received sign off by the authorized executive? | | | |
| The policy has been socialized across the Agency for personnel awareness. | Has the policy been shared with all personnel across-Agency? | | | |
| Documented Asset Management Policy. | Does your Agency have a documented Asset Management Policy? | | | |
| | Is the policy aligned with the State of South Carolina Asset Management Policy? | | | |
| Implemented Asset Management Policy and associated processes | Have you implemented an Asset Management Policy? | | | |
| | Do you have asset management processes implemented in your Agency? (i.e. asset inventory creation and review, asset registration, asset classification, user provisioning, etc.) | | | |

1 Policy Requirement and Questions

The Policy Requirements in the first column are based on the provisions/clauses stated in the respective policy. The Questions in the second column are simplified versions of the specific clauses to guide users in understanding the overall intent of the requirement.  Answering these questions may help an agency determine the existing gaps or areas where agencies can improve on current processes and procedures. When in doubt, refer back to the policy itself and read the related requirement.

2 Document Agency Response

Agencies are to document the response to the questions in Column 3. The response to the Questions column may be “Yes”, “No”, “N/A” and “Partial”. The goal is to help agencies identify areas or processes to be developed or improved in order to meet the requirements stated in the policy. Agencies are advised to use “Partial” for processes which are not completely implemented or documented. For instance, an agency might have an informal process in place which is performed but not documented, or the process doesn’t fully satisfy the clause in the gap analysis. For many of the questions in the gap analysis, a “No” or “Partial” response may mean that there is a gap to be remediated. It should be noted that gaps are not consistently indicated by a “No” response.  There are some questions in the gap analysis templates where

"Yes" may mean there is a gap. An example is from the Access Control Gap Analysis, "Does the Agency allow wireless access points to be installed independently by users?" If there is no gap, the answer to that question would be "Yes".

3 Document Gaps and Comments

Agencies are required to document the gaps after providing the responses to the questions. The Gaps column is where the agency documents the gaps identified. Gaps should be documented in detail, so that each gap can be understood as a stand-alone statement. The gaps identified during this process will go directly into the "Current Gaps" Column of the Implementation Plans, hence it is important that each gap is detailed enough to be a stand-alone statement. Agencies may add multiple gaps per question, so that each of these gaps may be addressed separately. It is recommended to separate out process and documentation gaps (see challenges below) in the gaps section, as the effort to remediate documentation and process gaps are different and may help agencies prioritize the remediation activities. The last column, Comments, is for the agencies to document comments about the current environment, notes about current processes, or notes on how to proceed with the implementation plan. It is recommended that agencies document as many comments on the current environment as possible before finalizing the gap. In addition, as the gap analyses are meant to be completed once as a point in time exercise, the more comments that can be captured, the better reference points you will have for the implementation team.

For further details and challenges associated with the Gap Analyses, refer to Appendix D.

### 2.2.3. Document Policy Implementation Plan

Building and documenting an implementation plan is the last sub-step of the InfoSec Policy Analysis step. The implementation:

- Helps the agency develop specific remediation activities and a Plan of Action and Milestones (POA&M) to address the identified gaps identified in the previous sub-step.
- Helps the agency define specific owners for each remediation activity in the implementation plan or specific owners for each step in the remediation process.
- Helps the agency identify challenges that are being faced (or that may be faced in the future) by the agency while performing the remediation activities.

The implementation plans are meant to be a living document, meaning they are designed to be constantly updated based on the changing circumstances, tackled challenges, completed remediation activities, and other evolving situations within the agency. In accordance to the deadlines set by DIS, agencies need to have fully documented their implementation plans by January 31st, 2015.

The following section outlines the approach that an agency can follow to develop and document the implementation plans, based on the gap analyses conducted for the thirteen state policies. Agencies may create thirteen separate implementation plans for each of the thirteen policies or one consolidated implementation plan incorporating the gaps from the thirteen policies. A sample template that illustrates a completed Implementation Plan for Asset Management can be found in Appendix E - Sample Implementation Plans – Asset Management in the Information Security Policy Handbook Appendices document.

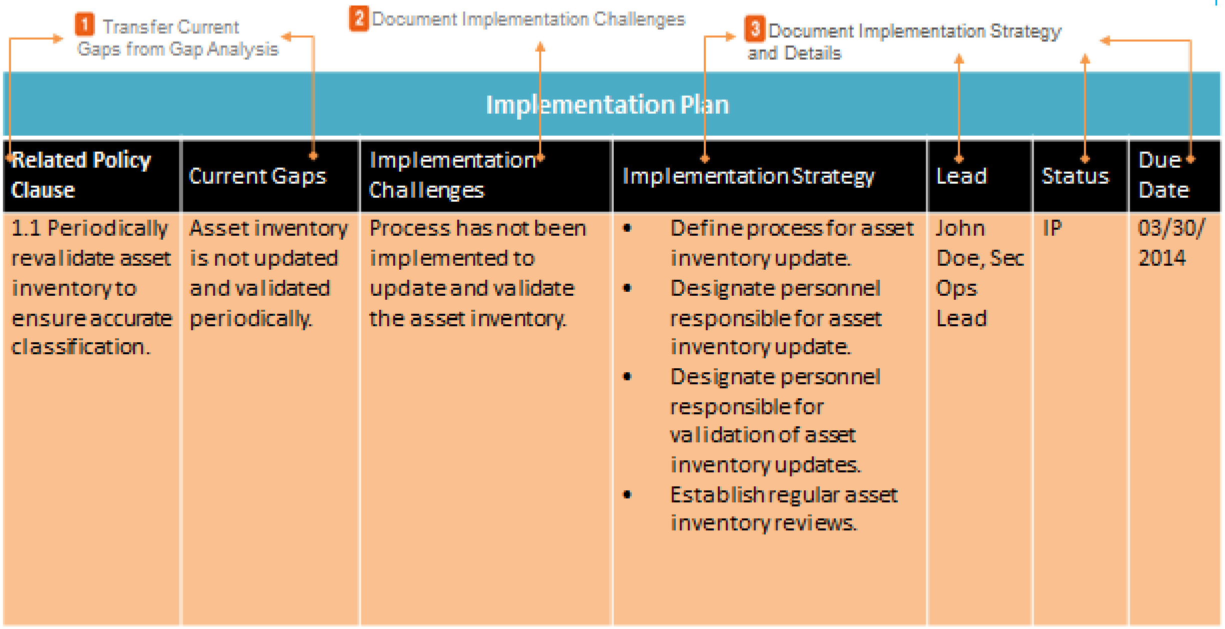
## *Approach for Implementation Plan*

The implementation plan template has been published and can be found on the DIS Website (http://dis.sc.gov/resources). Agencies are free to tailor the implementation plan as required; they can even migrate it to an excel spreadsheets and add additional columns as required. The implementation plans are to be made based on the gap analyses performed by the agency.

Figure 4 below shows general guidelines on how to use the implementation plan template and how to develop the implementation plan.

**Figure 4. Components of the Implementation Plan Template**

Implementation Plan - Template



1 Transfer Current Gaps from Gap Analysis

2 Document Implementation Challenges

3 Document Implementation Strategy and Details

| Implementation Plan | | | | | | |
|---|---|---|---|---|---|---|
| **Related Policy Clause** | **Current Gaps** | **Implementation Challenges** | **Implementation Strategy** | **Lead** | **Status** | **Due Date** |
| 1.1 Periodically revalidate asset inventory to ensure accurate classification. | Asset inventory is not updated and validated periodically. | Process has not been implemented to update and validate the asset inventory. | • Define process for asset inventory update.<br>• Designate personnel responsible for asset inventory update.<br>• Designate personnel responsible for validation of asset inventory updates.<br>• Establish regular asset inventory reviews. | John Doe, Sec Ops Lead | IP | 03/30/2014 |

1 Transfer Current Gaps from Gap Analysis

Agencies should transfer the gaps from the gap analysis directly to the implementation plan, as the starting point of the exercise. The second column, Current Gaps, is the finalized gaps from the gap analysis. The first column, Related Policy Clause, refers to the related policy clause, and can be identified as the policy itself, policy section, policy clause from the gap analysis, or the actual text of the requirement. If multiple gaps are identified for the same policy clause, it is recommended to have separate entries for each, as it will help with tracking and remediating each gap independently.

2 Document Implementation Challenges

The third column in the implementation plan template can be used by agencies to document challenges that are faced. It may refer to challenges that are present currently or to something that the agency foresees in the future or while performing the implementation (e.g. lack of professional skills, budget, resources, waiting for response to an RFP). There may be a cases where, in order to remediate a gap, another remediation has to be completed, so the challenge may be as simple as waiting for remediation of the gap. For instance, when there is a need for process redesign and documentation related to the same policy clause, the documentation gap can only be remediated once the process gap has been, so an agency may document “Need remediation of process gap” as a challenge. Challenges are meant as a brainstorming exercise.

3 Document Implementation Strategy and Details

Agencies are required to document the implementation strategies to remediate the gaps identified. The forth column referred as “Implementation Strategy” may be used to document the steps involved in the remediation strategy. The strategy may be identified as short term, medium term, or long term. For instance, a short term strategy for a gap in patch management may be as simple as “Waiting for State solution for Patch Management”. The long term strategy can to be built out once the state has announced the available solution. The fifth column referred to as “Lead” refers to the team, or person in charge of leading the remediation activities. The agency may also add a priority column, to fix some gaps before others depending upon the priority assigned by discussing with the stakeholders. Agencies are also advised to track the status of the remediation activities; the sixth column “Status” may be used to track this. Agencies should also define a due date for each of the remediation activities; it may be updated in the last column of the implementation plan template. Agencies are advised to use individual due dates for each remediation activity.

For further details and challenges associated with the Implementation Plans, refer to Appendix E.

## 2.3. Step 2 – InfoSec Executive Management Approval & Policies Implementation

### *Executive Management Review and Approval*

After completing the InfoSec Policies Analysis step, an agency should have a singular or set of implementation plans designed to address how they will overcome the gaps identified against the thirteen state policies. The important goal as part of step 2 is to obtain executive management approval for how the agency plans on implementing strategies (implementation plan) to address the information security gaps. The agency should design or utilize an existing review process to help management reviews of the policies, processes, and supporting documentation associated with the remediated gaps. The process should be a continual loop of reviewing the policies (and supporting documentation if applicable), changes suggested or identified, edits made based on changes, and back to review again, until the policies are ultimately approved.

Executive management approval allows the message to be passed from the top of the organization down to each of the employees. In addition, leadership can provide a high level perspective on budget, allocation of resources, priorities for implementation. Throughout the process, executive management should play a leading role in the determination of the implementation plan, as should have been identified on the Roles and Responsibilities Chart, column 'Revision and Approval'.

## 2.4. Step 3 – InfoSec Policies Awareness

The final step in in the process is policy awareness and training for agency personnel, for new and revised processes, and for solutions implemented. Agency personnel must be informed and trained on new security requirements, as they apply to job duties. While the implementation of policies can be incremental between now and July 1, 2016, over the course of the workstream, the following are different strategies agencies are using or to provide policy awareness and training. A combination of strategies may be applied as appropriate to an agency's circumstances.

- ***Intranet Posting*** **–** New and revised policies and procedures should be posted internally to allow agency personnel the chance to review the policy at a given point. **Avoid posting internal policies and procedures on publicly accessible servers, as this information might be used by criminals to gain insider knowledge and advantage in finding security weaknesses.**
- ***Security Slogan*** – An innovative approach revealed by several agencies was the introduction of a security slogan to help enforce the premise of consistently thinking about security during daily operations and normal business activities.
- ***Annual Employee Evaluation*** **–** Some agencies have found it effective to incorporate training for certain implemented requirements in the annual employee review process.
- ***Email*** – Agencies can use email announcements to target a specific section of the policy to a specific audience, to share a new requirement, providing fast and targeted awareness.

- ***Lunch & Learn Meetings*** – Introduce a series of training meetings over lunch, taking advantage of a more relaxed atmosphere.
- ***On-The-Job Training*** – One of the more effective ways for employees to learn and retain new security requirements is by learning on the job during daily operations.
- ***Online Training*** – Online training is another effective means to train employees on security requirements.
- ***Certifications*** – Agency leadership and training coordinators may encourage employees to obtain training and certifications.
- ***Security Seminar*** – Similar in nature to an 'All Hands Meeting,' an internal security seminar could be conducted.
- ***Newsletter*** – Another simple idea multiple agencies have begun to implement is to insert a particular policy requirement into a newsletter already issued by the agency.
- ***Training & Materials Availability*** – As much as possible, based on the type of training requirement, security training and awareness materials, presentations, and training modules should be available to agency employees for quick reference.
- ***Tiered Approach*** – With any of the delivery methods, a tiered approach may be considered, training on topics incrementally course of a year or more, so that all topics are covered by the compliance date of July 1, 2016.
- ***Pictorial Procedures*** – Procedures do not necessarily have to be documented entirely in text. Depending on the nature of the process, pictures can be used to aid employees in understanding processes, and to show a tangible example of how the process works in real life.

# 3. Additional Information

To supplement the SC Information Security Policy Handbook, each of the sections outlined in this document are further expanded with explanations, examples, and sample deliverables in the ***SC Information Security Policy Handbook Appendices***. In addition to the expansion of guidance on the handbook sections, a lessons-learned appendix is included to assist policy champions with common challenges and ways to think through solutions. The following is the breakdown of the appendix structure:

Appendix A – Policy Guidance & Training Initiative

Appendix B – Overview and Background

- Statewide Information Security Policies
- Information Security Policy Overview
- Policy Adoption Preparation
- Information Security Policy Deployment Additional Guidance
- InfoSec Policies Awareness

Appendix C – Sample Roles and Responsibility Chart

Appendix D – Sample Gap Analysis – Asset Management

Appendix E – Sample Implementation Plan – Asset Management

Appendix F – Lessons Learned: Information Security Policy Deployment

- InfoSec Policies Development Strategies
- Detailed InfoSec Policies Overview

Appendix G – Information Security Plan Development Guidelines (from DIS)