SOUTH CAROLINA
DEPARTMENT of ADMINISTRATION

SOUTH CAROLINA STATEWIDE INFORMATION SECURITY PROGRAM POLICY

January 1, 2026

Revision History

Version Number	Date	Author(s)	Description
1.0	March 7, 2014	Division of Information Security	Initial draft.
1.1	March 25, 2014	Division of Information Security	Establish implementation timeline; refine titles and duties. Add Controls Deployment section.
1.2	June 13, 2014	Division of Information Security	Established implementation timeline for Information Security Controls Deployment.
2.0	January 1, 2026	Division of Information Security	Complete revision to bring in alignment with current legislative requirements. Document title changed from “Information Security Program Master Policy.”

Contents

I. INTRODUCTION

The South Carolina General Assembly has authorized the South Carolina Department of Administration's (Admin) Division of Information Security (DIS) to establish a statewide information security program.

This program policy describes the structure, governance and scope of the South Carolina Statewide Information Security Program (SC InfoSec Program) and the organizational roles and responsibilities shared between state agencies and DIS in matters relating to cybersecurity. (In this policy and throughout the SC InfoSec Program, the terms information security and cyber security, cybersecurity or cyber are treated as synonymous.)

1. PURPOSE

The purpose of this policy is to establish the South Carolina Information Security Program, including its authority, scope, objectives, implementation and governance by defining the shared roles and responsibilities between DIS and the state agencies that safeguard state and citizen information.

2. AUTHORITY

The SC InfoSec Program and associated requirements set forth in this policy are based on legislative authorities established by the South Carolina General Assembly in Provisos 93.9, 117.96, 117.102 and 117.107 of the 2025 General Appropriations Act.

3. SCOPE

This policy and the SC InfoSec Program standards, policies and guidelines apply to all South Carolina state government agencies with the following exceptions derived from the legislative authorities referenced above.

a. Exempt: Judicial and Legislative Branch Agencies

The following state entities are exempt from this policy and the SC InfoSec Program:

- The South Carolina Judicial Branch
- The South Carolina House of Representatives
- The South Carolina Senate
- Legislative Council
- Legislative Audit Council
- Legislative Services Agency
- Judicial Department

Note: The terms "state agencies" and "all state agencies," as used in this policy and in all SC InfoSec Program materials, shall always be understood to ***exclude*** *the judicial and legislative branch agencies listed in this section, unless they are explicitly included by additional clarifying language*.

All South Carolina government entities exempt from this policy and the SC InfoSec Program are encouraged to review and evaluate the policies, standards, guidelines

and other requirements contained within the program and adopt or adapt for their own use as appropriate.

b. <u>Modified Obligation: Public Institutions of Higher Learning, Technical Colleges, Quasi-Governmental Bodies and Political Subdivisions</u>

The following state agencies are included within the scope of this policy and SC InfoSec Program requirements; however, they are exempt from mandatory adoption of shared information technology and infrastructure services, from submitting IT Security Plans to DIS and from DIS audits of program compliance. (In lieu of an audit, DIS may request an agency provide compliance evidence.)

Public Institutions of Higher Learning and Technical Colleges:

- Aiken Technical College
- Central Carolina Technical College
- Clemson University
- Coastal Carolina University
- College of Charleston
- Denmark Technical College
- Florence Darlington Technical College
- Francis Marion University
- Greenville Technical College
- Horry-Georgetown Technical College
- Lander University
- Medical University of South Carolina
- Midlands Technical College
- Northeastern Technical College
- Orangeburg-Calhoun Technical College
- Piedmont Technical College
- SC State University
- Spartanburg Community College
- Technical College of the Lowcountry
- The Citadel
- Tri-County Technical College
- Trident Technical College
- University of South Carolina (including all divisions, departments, schools and colleges)
- University of South Carolina – Aiken
- University of South Carolina – Beaufort
- University of South Carolina – Lancaster
- University of South Carolina – Salkehatchie
- University of South Carolina – Sumter
- University of South Carolina – Union
- University of South Carolina – Upstate
- Williamsburg Technical College
- Winthrop University
- York Technical College

Quasi-Governmental Bodies:

- Connector 2000 Association
- Palmetto Railways
- SC Jobs-Economic Development Authority
- SC Lottery Commission
- SC Public Service Authority (Santee Cooper)
- SC Research Authority
- SC State Education Assistance Authority
- SC State Ports Authority

Political Subdivisions:

For purposes of the SC InfoSec Program, political subdivisions are all counties, municipalities, school districts and public service or special districts.

II. POLICY STATEMENTS

1. PROGRAM OBJECTIVES

The SC InfoSec Program shall be a statewide mechanism for developing, implementing, adopting and monitoring information security capabilities across state government.

The program shall be a collaborative effort between DIS and state agencies wherein responsibility for information security is shared. DIS shall provide both information security leadership and support in service of state agencies while they retain overall accountability for their own information security as they independently pursue their individual mandates in service of the state and its citizens.

- The activities within the SC InfoSec Program shall fall broadly into four categories:
  - Continuous assessment of information security risk.
  - Iterative development of information security requirements to mitigate information security risk.
  - Collaborative implementation of information security requirements.
  - Regular monitoring of compliance with information security requirements.
- Neither DIS nor state agencies shall be wholly responsible for any of these activities; they shall be jointly performed as DIS works in partnership with state agencies through a shared responsibility model. By sharing responsibility for information security, both parties partner to enable agencies to fulfill their mandates with minimal information security risk.
- Implementing a properly balanced shared responsibility model for statewide information security shall be a primary objective of the SC InfoSec Program. Each agency is accountable for its own mandate, mission, vision, objectives, federal and state compliance burden, and risks (including business, operational and information security risks). DIS is accountable to provide information security leadership and services to South Carolina state government in accordance with legislative requirements. There is therefore a shared responsibility for state

government information security between DIS and agencies. The SC InfoSec Program shall be the means for that shared responsibility for information security to be implemented.

A high-level view of the elements of the SC InfoSec Program and the governance relationships between them are pictured below. The objectives of the program are described in the following sections.

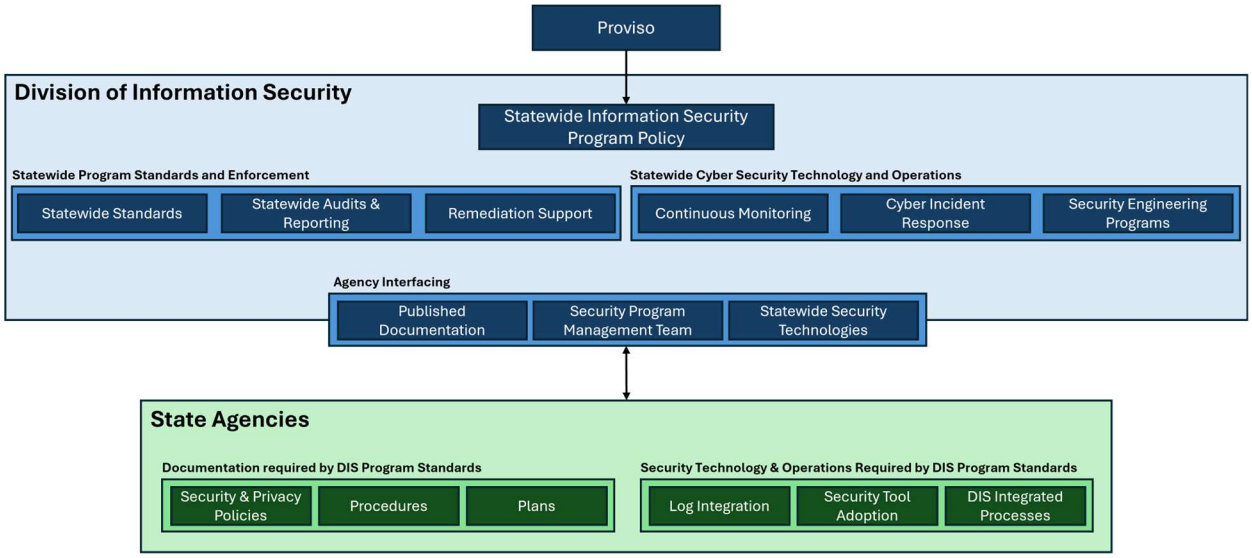

Figure 1: The Statewide Information Security Program

a. Collaborative Information Security Governance

A fundamental purpose of the SC InfoSec Program is to provide a common information security framework and approach across state government. At its heart, the program is a governance effort — a collaboratively-developed collection of policies, standards, guidelines and other elements that enable all in-scope state government agencies to approach information security in a uniform manner, collectively improving the state's information security posture while ensuring each agency's independence to pursue its mission, goals and objectives.

DIS contributes to statewide information security governance by developing information security policies, standards and guidelines in collaboration with state agencies, ensuring they are regularly updated and maintained, and by monitoring and reporting on levels of information security risk and levels of compliance with information security requirements within state government. In addition, DIS supports agencies by providing subject matter expertise and support in information security governance and compliance activities when requested.

All state agencies contribute to statewide information security governance by contributing to the development of information security policies, standards and guidelines, implementing information security in accordance with those requirements and partnering with DIS to respond to information security risk and incidents.

b. Integrated Information Security Requirements

The information security requirements established by the SC InfoSec Program are multifaceted. Some are deeply technical; others are process focused. Some focus on documentation; others focus on tools and operations. Some are preventive; others are responsive. Despite this variety, program requirements are integrated with one another into a single, holistic structure that provides traceability across the whole program — from requirement to authority, from risk to mitigation and from policy requirement to technical standard.

Notable aspects of the program's integrated requirements include:

- SCDIS-200 Information Security and Privacy Standards.
- Domain-specific information security policies that align with SCDIS-200 controls.
- SCDIS-210 technical information security standards that align with SCDIS-200 controls.
- Information security tools that meet the technical standards.
- Information incident response plans that align people and processes with the information security tools.
- Information security risk assessment activities that align with both technical and policy requirements.

Information security requirements developed as part of the SC InfoSec Program are developed and published by DIS in collaboration with state agencies as information security policies, guidelines and standards. All such requirements exist and operate under the authority of this program policy.

Publicly available SC InfoSec Program requirements are published to the Admin website. Confidential information related to the SC InfoSec Program is shared with authorized individuals through the DIS governance, risk and compliance (GRC) platform or upon request.

c. Right-Sized Information Security Technology Enablement

Information security technologies enabling automated detection and response are essential to a modern, effective information security program. Through the SC InfoSec Program, DIS partners with in-scope agencies to govern, design, procure and implement information security solutions that are best fit for the state and each agency's needs.

Governance of information security technologies is implemented by means of information security policies, standards and guidelines that establish a minimum information security technology baseline, and which must be met or exceeded by all state agencies subject to SC InfoSec Program requirements.

Some information security solutions are designed, procured and implemented by DIS for use by all in-scope state agencies as a centralized service. Adoption of such solutions is a mandatory obligation for all state agencies subject to Admin's shared services authority under legislative proviso. In addition, a portion of the DIS budget has been designated by the General Assembly for the distribution of information security

technologies to state agencies (even those exempt from shared services obligations) to address the state's most serious information security vulnerabilities as determined by DIS and Admin's Office of Technology and Information Services (OTIS).

As part of the SC InfoSec Program, DIS also offers information security technology support services such as risk assessments and design and engineering services.

d. Coordinated Cyber Incident Response

In the event of a cyber incident or breach, a rapid and skillful response is essential to minimize any potential damage or impact on the state, its agencies and its citizens. Ensuring all state agencies have timely access to high-quality, effective cyber incident response resources is a primary driver for the SC InfoSec Program.

Some aspects of information security incident management are centralized across the state by DIS. DIS provides one statewide security information and event management (SIEM) system and one statewide Security Operations Center (SOC). DIS promulgates a statewide cyber incident response plan. However, in partnership with these centralized capabilities, each state agency also develops its own cyber incident response plans and capabilities.

In the event of a cyber incident, DIS oversees cyber incident response under the SC InfoSec Program with the level of engagement and direct oversight determined by DIS in partnership with the affected agency(ies) to be most prudent. The end goal is always the same: a collaborative and well-coordinated defense of the state, its interests and its citizens.

e. Transparent Cyber Risk Management

In the state government context, apportionment of resources and prioritization of effort is based on a collaborative, iterative legislative process. Providing decision makers with clear visibility to accurate, up-to-date information about the presence and urgency of information security risks and the effort needed to mitigate those risks is a key objective of the SC InfoSec Program. Decision makers at both the agency and the state level benefit from a clear, apples-to-apples picture of sources of information security risk within their scope. This enables them to prioritize efforts and investments in a manner best serving the interests of the state and its citizens.

The SC InfoSec Program provides a single cyber risk management framework for use across all state agencies. This single framework allows all information security risks to be identified, assessed, tracked and managed in a consistent and coordinated manner, putting priority where it is needed most.

2. PROGRAM COMPONENT REQUIREMENTS

The SC InfoSec Program shall consist of five types of components. The policy requirements for each are provided in the following sections.

a. Sub-Programs

- The SC InfoSec Program shall be structured into distinct, individually governed sub-programs. This modular approach ensures each area can mature and

update at its own pace while allowing for more effective distribution of roles and responsibilities.

- Each sub-program shall be established and governed by its own program policy which shall exist and operate under the overarching program policy authority.
- The current sub-programs of the SC InfoSec Program are:
    - The Security and Privacy Compliance Program
    - The Cyber Risk Management Program
    - The Security Engineering and Operations Program
    - The State Agency Security Engagement Program
    - The Enterprise Privacy Office Program

b. Policies

- Information security policies shall be the highest-level of governance within the SC InfoSec Program.
- Policies shall be published as signed, versioned documents.
- Standards, guidelines and services within the program shall be governed by and must align with program policies.
- Policies shall be developed by DIS in collaboration with state agencies and approved by the DIS Chief Information Security Officer (CISO).
- Policies shall be published to authorized individuals through the DIS GRC platform and at the discretion of the DIS CISO on the Admin website.
- Policies shall be reviewed and updated in a manner and at a cadence documented in each individual policy.

c. Standards

- Information security standards shall be the second level of governance within the SC InfoSec Program.
- Standards shall guide and enable the implementation of policy requirements.
- Standards shall address a variety of topics, including technical, process and governance matters.
- Standards shall be promulgated in a variety of forms, such as process or procedure documents, plans, tabular lists, configurations within systems, presentation slides and other such forms.
- Standards shall be developed by DIS in collaboration with state agencies and approved by the DIS CISO or persons authorized by the DIS CISO.
- Standards shall be published in a manner and to an audience deemed appropriate by DIS.
- Standards shall be reviewed and updated in a manner and at a cadence that complies with SC InfoSec Program policies.

d. Guidelines

- Guidelines shall be the lowest level of governance within the SC InfoSec Program.
- Guidelines shall support the implementation of standards by providing recommendations and guidance.
- Guidelines shall address a variety of topics, including technical, process and governance matters.
- Guidelines shall be promulgated in a variety of forms, such as formal documents, tabular lists, configurations within systems, presentation slides and other such forms.
- Guidelines shall be developed by DIS in collaboration with state agencies and approved by DIS staff.
- Guidelines shall be published to authorized individuals in the manner deemed most appropriate by DIS.
- Guidelines shall be reviewed and updated in a manner and at a cadence determined by DIS.

e. Services

- SC InfoSec Program services shall be technology or consulting services offered by DIS to state agencies to support them in their implementation of SC InfoSec Program requirements.
- Adoption of some services as defined by DIS shall be mandatory for all in-scope agencies.
- Adoption of other services, as defined by DIS, shall be optional and may be utilized by agencies in a manner and at a cadence that best suits their needs and priorities.
- DIS shall develop services and make them available to agencies based on DIS priorities as defined through continual, collaborative engagement with state agencies.

3. PROGRAM GOVERNANCE

- The SC InfoSec Program shall be governed by this program policy in accordance with authorities conferred and requirements promulgated by the General Assembly as referenced in Section 2 of this policy.
- The constituent parts of the SC InfoSec Program shall be governed by the various information security policies, standards and guidelines created as part of the SC InfoSec Program.

4. PROGRAM IMPLEMENTATION

- DIS shall outline activities, projects, programs, phases and milestones by which the SC InfoSec Program will be implemented and maintained.
- DIS shall define SC InfoSec Program implementation priorities and plans in coordination with state agencies.

5. ROLES AND RESPONSIBILITIES

The SC InfoSec Program shall be a coordinated effort between DIS and state agencies as outlined below.

a. SC DIS

DIS shall:

- Develop, implement, update and maintain the SC InfoSec Program as a collaborative effort between DIS and state agencies.
- Provide information security leadership and support to state agencies through the SC InfoSec Program as they independently pursue their individual mandates.
- Develop, implement, update and maintain sub-programs and services in collaboration with state agencies as part of the SC InfoSec Program.
- Develop, implement, update and maintain information security policies, guidelines and standards in collaboration with state agencies as part of the SC InfoSec Program.
- Ensure all requirements of the SC InfoSec Program integrate with one another into a single, cohesive body of work.
- Conduct audits of state agencies (except for public institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies) as necessary to monitor compliance with established information security policies, guidelines and standards.
- As needed, request public institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies to submit sufficient evidence that their information security policies, guidelines and standards meet or exceed those adopted and implemented by the SC InfoSec Program.
- Ensure documentation is acquired and recorded for all reported state agency information security breaches.
- Oversee information security incident response for state agencies in the manner deemed most prudent by DIS.
- Use funds for enterprise technology and remediation to address the state's most serious information security vulnerabilities as determined by DIS and OTIS.
- Partner with OTIS to provide shared information technology and infrastructure services that promote information security to state agencies (except for public

institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies).

- Determine the sequence of statewide information security technology and service provisioning.
- Coordinate with agencies to accomplish a strategic transition to statewide information security technologies and services.
- Specify the form and level of detail required in state agency IT security plans submitted to DIS.
- Annually review all state agency IT security plans (except for public institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies).
- Partner with state agencies to govern, design, procure and implement information security solutions, technology and services.
- Provide a single cyber risk management framework for use across all state agencies.
- Assess, track and oversee the management of information security risk across state agencies.

b. State Agencies

All state agencies shall:

- Adopt and implement information security policies, guidelines and standards promulgated by DIS.
- Formally report all information security breaches to DIS and provide or assist with developing related documentation as requested.
- Be subject to DIS oversight of information security incident response in the manner deemed most prudent by DIS.
- Use enterprise technology and remediation distributed to state agencies by DIS to address the state's most serious information security vulnerabilities as determined by DIS and OTIS.

State agencies with full obligation (agencies that are not public institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies) shall:

- Fully participate in information security audits conducted by DIS that monitor compliance with established information security policies, guidelines and standards.
- Use the shared information technology and infrastructure services provided by DIS as they become available and in a sequence determined by DIS.
- Coordinate with DIS to accomplish a strategic transition to shared information security services.

- Submit an IT Security Plan to DIS in the form and level of detail required by DIS by August 1 of the fiscal year.

State agencies with modified obligations (public institutions of higher learning, technical colleges, political subdivisions and quasi-governmental bodies) shall:

- Submit sufficient evidence upon request from DIS that their information security policies, guidelines and standards meet or exceed those adopted and implemented by the SC InfoSec Program.

III. POLICY GOVERNANCE

1. POLICY DEVELOPMENT

This policy was developed by DIS to meet the requirements established by the General Assembly in the authorities referenced in Section 2. It provides the information required to develop, implement and maintain a statewide information security program.

2. POLICY DISTRIBUTION

The Admin Strategic Communications Office shall ensure the latest approved version of this policy is posted to the Admin website and emailed to state agencies and other stakeholders as appropriate.

3. POLICY MAINTENANCE

DIS shall maintain this SC InfoSec Program Policy, and shall:

- Perform a formal review and renewal every fiscal year.
- Include appropriate staff members, stakeholders and state agency representation in the review and renewal process.

4. POLICY EXCEPTIONS

All SC InfoSec Program requirements are mandatory for in-scope agencies. Exceptions to program requirements are only available when external constraints beyond an agency's control (such as conflicting legislative mandates or compliance burdens) prevent an agency from meeting program requirements.

- State agencies shall request exceptions when external constraints prevent the fulfillment of specific policy requirements.
- DIS shall establish and implement a process for agencies to request exceptions, approval criteria for exceptions and expiration of exceptions.

5. POLICY AUTHORIZATION

As the state official responsible for the fulfillment of DIS's legislative mandate, including the development and implementation of a statewide information security program, this policy is authorized by the State Chief Information Security Officer.

Date of Original Issue: March 7, 2014
Date of Current Revision: January 1, 2026
Current Revision Number: 2.0

Authorized by: Ben Willis
State Chief Information Security Officer
Division of Information Security
South Carolina Department of Administration

Date