STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 1 – Information Security Master

Chief Information Security Office

March 2020

Introduction

SCDE Organizational and Functional Responsibilities

The policy sets the minimum level of responsibility for the agency, staff, contractors and third parties.

SCDE Chief Information Security Office (CISO)

The duties of the Chief Information Security Office are

- developing, maintaining, and revising information security policies, procedures, and recommended technology solutions; and
- providing technical assistance, advice, and recommendations concerning information security matters.

South Carolina Department of Education

Information security is an SCDE responsibility shared by all members of the SCDE senior staff, as well as all employees of the SCDE. The senior staff shall provide clear direction and visible support for security initiatives. The SCDE 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 adherence to agency policies, regulatory compliance, and risk mitigation strategies;
- 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, and
    - determining when to retire or purge the data.

SCDE Employees, Contractors, and Third Parties

All SCDE 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; and
- being accountable for their actions relating to their use of all State information systems.

Purpose

- These policies exist in addition to all other SCDE policies and federal and state regulations governing the protection of SCDE data. Adherence to the policies will improve the security posture of the State and help safeguard SCDE information technology resources.

Policy Section Overview

Each information security policy section consists of the following:

- Purpose: Provides background to each area of the information security policies.
- Policy Controls: Provides the internal policy number and the policy control.
- 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 Master Policy Controls

1.100 Information Security Program Planning

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.

Policy ID	Control Description
1.101	The SCDE 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.
1.102	The SCDE'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.
1.103	The SCDE shall ensure coordination among the agency's business units responsible for the different aspects of information security (e.g., technical, physical, personnel)
1.104	The SCDE shall ensure that senior staff approve the security plan.
1.105	The SCDE shall review the information security plan at least on an annual basis.
1.106	The SCDE shall update the security plan to address changes and problems identified during plan implementation or security control assessments.
1.107	The SCDE shall protect the information security plan from unauthorized disclosure and modification.
1.108	The SCDE shall consider resources needed to implement and maintain the information security plan in capital planning and investment requests.
1.109	The SCDE shall implement a process for ensuring that plans of action and milestones for the security program and associated information systems are developed and maintained.
1.110	The SCDE shall review plans of action and milestones for consistency with the agency's risk management strategy and priorities for risk response actions.

Policy ID	Control Description
1.111	SCDE must develop, monitor, and report on the results of information security and privacy measures of performance to agency head.

1.200 Security Organization (Roles and Responsibilities)

The purpose of this section is to establish key principles based on which the SCDE's Security Organization shall be established.

Policy ID	Control Description
1.201	The SCDE's Superintendent shall ensure that the agency's senior staff are given the necessary authority to secure the operations and assets under their control.
1.202	The SCDE shall appoint an information security liaison with the mission and resources to coordinate, develop, implement, and maintain an information security plan.
1.203	The SCDE shall establish an information security workforce and professional development program appropriately sized to the agency's information security needs.
1.204	The SCDE shall provide role-based security training to personnel with assigned security roles and responsibilities.

1.300 Policy Management

The purpose of this section is to establish key principles based on which the SCDE's security procedures shall be developed.

Policy ID	Control Description
1.301	The SCDE 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.
1.302	The SCDE shall allocate the appropriate subject matter experts to the development of State and agency-specific information security procedures.
1.303	The SCDE 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.

Policy ID	Control Description
1.304	The SCDE 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.
1.305	Information security procedures that are developed at the agency shall contain the following information, as appropriate: • revision history; • introduction; • preface; • ownership, roles, and responsibilities; • purpose; • policy statements; • policy supplement; • guidance; and • definitions.
1.306	The SCDE shall review each draft procedure with stakeholders who shall be impacted by the procedure to ensure that the procedure is enforceable and effective.
1.307	The SCDE 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.
1.308	The SCDE 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.
1.309	A procedure governance committee shall be established for the purpose of review and approval of procedures.
1.310	The SCDE 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.
1.311	The SCDE shall require employees to review and acknowledge understanding of information security procedures prior to allowing access to sensitive data or information systems.

1.400 Information Security Controls Deployment

The purpose of this section is to establish key principles for deployment of information security controls.

Policy ID	Control Description
1.401	The SCDE shall adopt a risk-based approach to prioritize deployment of controls.
1.402	The SCDE shall allocate the appropriate subject matter experts to the deployment of State and agency-specific information security controls.
1.403	The SCDE 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.
1.404	Controls which cannot be deployed due to the agency's resources or other constraints must be reported to the office of the State Chief Information Security Officer.
1.405	The SCDE shall review each control with stakeholders who shall be impacted to ensure that the control is enforceable and effective.
1.406	The SCDE shall develop and implement a communication plan to disseminate new controls or changes to existing controls.
1.407	The SCDE must periodically review information security controls, staging each full review cycle across no more than a 3-year period.

Policy Supplement

Refer to the SCDIS-200-InformationSecurityandPrivacyStandards030717.xlsx located in the SCDE Info Sec policy folder.

Guidance

NIST SP 800-53 Revision 4: Security and Privacy Controls for Federal Information Systems and Organizations

Reference

National Institute of Standards and Technology (NIST) see NIST SP 800-53 Revision 4