STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 4 — Risk Management

Chief Information Security Office

February 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.

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).

Risk Management - Policy Controls

4.100 Risk Management

The purpose of the risk management section is to define the controls that shall be implemented by the SCDE to identify and assess information security risks and to take steps to reduce risk to an acceptable level.
Risk management typically consists of the following:

- 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 ID	Control Description
4.101	The SCDE shall define a schedule for an on-going risk assessment and risk mitigation process.
4.102	The SCDE shall review and evaluate risk based on the system categorization level and/or data classification of their systems.

4.200 Risk Assessment

The purpose of the risk assessment section is to define a process to identify and manage IT security risks to determine the extent of the potential threat and the risk associated with IT security.

Policy ID	Control Description
4.201	The SCDE 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.
4.202	The SCDE 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).
4.203	The SCDE shall ensure that risk assessments identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the SCDE
4.204	The SCDE shall develop and periodically update a Plan of Action & Milestones (POAM) document that shall identify any deficiencies related to internal

Policy ID	Control Description
	security controls. The POAM shall identify planned, implemented, and evaluated remedial actions to correct deficiencies noted during annual assessments.
4.205	The SCDE shall establish a process and assign a senior staff 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 SCDE shall make a decision regarding risk treatment.

4.300 Risk Mitigation

The purpose of the risk mitigation section is to support mitigation of risks identified and to define the level of risk that is acceptable to the SCDE where risks are accepted knowingly and objectively.

Policy ID	Control Description
4.301	The SCDE 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.
4.302	The SCDE 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 SCDE.

Policy Supplement

Refer to the SCDIS-200-InformationSecurityandPrivacyStandards030717.xlsx located in the SCDE InfoSec 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