STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 9 - IT Risk Strategy

Chief Information Security Office

January 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).

IT Risk Policy Controls

9.100 Security Performance and Metrics
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 ID	Control Description
9.101	The SCDE must monitor and report performance metrics to agency head to demonstrate progress in adoption of security controls, and associated policies and procedures, and effectiveness of the information security program.
9.102	SCDE must define performance measures to be able to support the determination of information system security posture, demonstrate compliance with requirements, and identify areas of improvement.
9.103	SCDE must ensure that the defined metrics are meaningful, yield impact and outcome findings, and are scheduled for collection with the time necessary for stakeholders to use the results to address performance gaps.
9.104	SCDE must standardize the data collection methods and data repositories used for metrics data collection and reporting to ascertain the validity and quality of data.

9.200 Third-Party Risk Management
The purpose of the Third-Party Risk Management section is to establish the controls to safeguard SCDE information and information processing facilities that are accessed, processed, communicated to, or managed by third parties.

Policy ID	Control Description
9.201	SCDE must establish processes to ensure that third parties comply with information security requirements and employ defined security controls in accordance with compliance requirements incumbent on the agency.
9.202	The SCDE must implement processes, methods, and techniques to review compliance by third parties on an ongoing basis.
9.203	The SCDE must establish a process to conduct risk assessments on third party service providers, and document the risk assessment results.
9.204	The SCDE must 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.

9.205 SCDE must authorize connections between agency information systems and third party information systems by entering into Interconnection Security Agreements.

9.206 The SCDE must ensure that for each third party system interface with an agency system, the interface characteristics, security requirements, and the nature of the information communicated are documented.

9.207 The SCDE agency must establish terms and conditions for trust relationships established with other entities owning, operating, or maintaining external information systems on behalf of agency. Terms and conditions should control:
- Access to agency information systems from third party information systems.
- Controls for processing, storing, or transmitting of agency data by third party information systems.

9.208 SCDE must review and update third party security agreements on an annual basis, or as defined in the contract.

9.209 SCDE must share personally identifiable information (PII) with third parties only for purposes in compliance with applicable statutes and regulations.

9.210 The SCDE 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.

9.211 SCDE must 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.

9.212 The SCDE must 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

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