STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 3 — IT Compliance

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).

IT Compliance - Policy Controls

3.100 Audit and Compliance Requirements

The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance with information security policies and standards at State agencies and institutions.

Policy ID	Control Description
3.101	The SCDE shall identify and document its obligations to applicable State, federal and other third party laws and regulations in relation to information security.
3.102	The SCDE shall periodically review or audit its users' and systems' compliance with security policies, standards, and procedures, and initiates corrective actions where necessary.
3.103	The SCDE shall document and report findings from compliance reviews or audits to agency leadership.
3.104	The SCDE shall establish formal, documented audit and accountability procedures.
3.105	The SCDE shall implement a process to periodically review and update the audit and accountability procedures.

3.200 Information systems audit controls

The purpose of the Audit and Compliance section is to establish controls and processes to help ensure compliance with information security policies and standards at State agencies and institutions.

Policy ID	Control Description
3.201	The SCDE shall implement audit procedures to help ensure that activities involving reviews or audits of operational systems are carefully planned to minimize the risk of disruptions to business processes.
3.202	The SCDE shall implement security controls to help prevent unauthorized access and/or access abuse of audit tools, where applicable.
3.203	The SCDE shall determine the type of events that are to be audited within information systems.
3.204	The SCDE shall include the audits within its annual audit plan.

Policy ID	Control Description
3.205	The SCDE senior staff shall ensure coordination between the audit function, information security function, and business functions to facilitate the identification of auditable events.
3.206	The SCDE information systems shall be enabled to generate audit records containing details to help establish what type of event occurred, when and where the event occurred, the source and outcome of the event, and the identity of any individuals or subjects associated with the event
3.207	The SCDE shall analyze information system audit records periodically.
3.208	The SCDE shall implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.
3.209	Each agency must perform correlation and analysis of information generated by security assessments and monitoring.
3.210	SCDE must allocate sufficient audit storage capacity to ensure compliance with audit log retention requirements.
3.211	SCDE must implement provisions for information systems to off-load audit records at regular intervals onto a different system or media than the system being audited.

3.300 Continuous Monitoring

SCDE must ensure that its security controls for information systems are effective.

Policy ID	Control Description
3.301	The SCDE shall employ assessment teams to monitor the security controls on an ongoing basis
3.302	The SCDE assessment teams shall be independent from operational or business functions, or hired third parties.
3.303	The SCDE shall develop a plan of action and milestones to document planned remedial actions to correct weaknesses or deficiencies identified as a result of internal/external risk assessments, security reviews, and/or audits

Policy ID	Control Description
3.304	The SCDE shall update its plan of action and milestones at least on a yearly basis and also based on the findings from continuous security monitoring activities.

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