STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 5 — Physical Environmental Security

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).

Physical and Environmental Security

5.100 Physical Access and Security

The purpose of the Physical Access and Security section is to establish controls to prevent unauthorized physical access to the SCDE information assets to protect them from damage, interruption, misuse, destruction and/ or theft.

Policy ID	Control Description
5.101	The SCDE shall establish formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
5.102	The physical and environmental protection policy and associated procedures must be reviewed and updated on an annual basis.
5.103	The SCDE shall develop, approve, and maintain a list of personnel with authorized access to the facility where information systems are physically located.
5.104	The SCDE shall establish a process to review, approve, and issue credentials for facility access.
5.105	The SCDE shall remove individuals from the facility access list when access is no longer required.
5.106	The SCDE control entry to / exit from the data center(s) and/or sensitive facilities using physical access control devices (e.g., keycard or keys) and/or security guard(s).
5.107	The SCDE shall maintain physical access audit logs for data center(s) and/or sensitive facilities entry/exit points.
5.108	The SCDE shall employ guards and/or alarms to monitor physical access points to the data center(s) where the information system resides 24 hours per day, 7 days per week.
5.109	The SCDE shall perform security assessments on an annual basis at the physical boundary of the data center(s) to check unauthorized exfiltration of information or removal of information system components.
5.110	The SCDE shall establish a process to escort visitors and monitor their activity within the data center(s) and/or sensitive facilities.

Policy ID	Control Description
5.111	The SCDE shall change combinations and keys at defined intervals, and when keys are lost, combinations are compromised, or individuals are transferred or terminated.
5.112	The SCDE shall control physical access to information system distribution and transmission lines within the data center(s) using physical access control devices (e.g., keycard or keys).
5.113	The SCDE shall place output devices in secured areas and in locations that can be monitored by authorized personnel, and allow access to authorized individuals only.
5.114	The SCDE shall review physical access logs at a defined frequency and upon occurrence of security incidents.
5.115	The SCDE shall maintain visitor access records to the data center(s) and/or sensitive facilities for a minimum of 1 year.
5.116	The SCDE shall establish processes to authorize, monitor, and control items entering and exiting the data center(s) and maintain records of those items.

5.200 Environmental Security

The purpose of the Environmental Security section is to define controls to protect SCDE information assets from damage, destruction and/ or interruption due to environmental factors such as fire, humidity, water, power outage, etc…

Policy ID	Control Description
5.201	The SCDE shall place power equipment and cabling in safe locations to prevent environmental and/or man-made damage and destruction.
5.202	The SCDE shall make available the capability of shutting off power to data center(s) during an incident.
5.203	The SCDE shall place emergency shutoff switches or devices at locations that can be accessed safely and easy by personnel during an incident.
5.204	The SCDE shall implement physical and logical controls to protect emergency power shutoff capability from unauthorized activation.
5.205	The SCDE shall implement uninterruptible power supply to facilitate transition to long-term alternate power in the event of a primary power source loss.

Policy ID	Control Description
5.206	The SCDE shall install and maintain fire detection and suppression devices that are supported by an independent power source.
5.207	The SCDE shall employ fire detection devices/ system that activate automatically and notify emergency personnel and defined emergency responder(s) in the event of a fire.
5.208	The SCDE shall employ an automatic fire suppression system if/ when the data center(s) is not staffed on a continuous basis.
5.209	The SCDE shall employ automatic temperature and humidity controls in the data center(s) to prevent fluctuations potentially harmful to processing equipment.
5.210	The SCDE shall employ temperature and humidity monitoring that provides an alarm or notification of changes potentially harmful to personnel or equipment.
5.211	The SCDE shall protect processing equipment from damage resulting from water leakage.

5.300 Disposal of Equipment

The purpose of the Disposal of Equipment section is to define the controls that shall be followed for disposal of information system equipment which contains SCDE information..

Policy ID	Control Description
5.301	The SCDE shall define and implement mechanisms for disposal of digital media and data storage devices.
3.302	The SCDE shall employ sanitization mechanisms with the strength and integrity commensurate with classification of data to be sanitized.
3.303	The SCDE shall establish processes for cleansing and disposal of computers, hard drives, and fax/printer/scanner devices.
3.304	The SCDE shall implement controls to track and verify sanitization of devices prior to disposal.

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