STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 7 - Mobile 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.

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).

Mobile Security Policy Controls

7.100 Mobile Security

The purpose of the mobile security section is to describe the minimum security policy for agency-owned mobile devices (mobile devices) used to access State data, including usage restrictions, configuration management, device authentication, and implementation of mandatory security software.

State business requirements may, on occasion, justify storing confidential data on mobile computing devices. It is the responsibility of the SCDE to recognize the associated risks and take the necessary steps to protect and secure their mobile computing devices.

Policy ID	Control Description
7.101	The SCDE only allows portable media devices when these are assigned and identified to an individual owner.
7.102	The SCDE only allows the use of portable media devices that allow sanitization.
7.103	The SCDE shall use mobile devices that have the ability to be remotely wiped/erased.
7.104	The SCDE shall develop usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
7.105	The SCDE CISO shall develop a list of approved mobile devices. Only approved mobile devices shall be allowed to access the SCDE's network and information systems.
7.106	The SCDE shall develop and apply adequate asset management procedures to all mobile devices.
7.107	The SCDE shall utilize the approved encryption standard for mobile devices.
7.108	The SCDE shall implement controls to centrally manage the installation of standardized operating system, applications, and patches on mobile devices.
7.109	The SCDE shall remove sensitive and confidential information from the mobile device before it is disposed.
7.110	The SCDE shall deploy administrative and technical controls to mitigate risks associated with lost or stolen mobile devices.

Policy ID	Control Description
7.111	In order to reduce risks associated with vulnerabilities in mobile devices, the SCDE shall implement controls for testing vendor-recommended patches, hot-fixes, or service packs before such changes are approved for installation; and a process to keep system hardware, operating system, and applications up-to-date with the approved system updates.
7.112	The SCDE shall ensure that each agency-issued handheld computing device is configured so that only approved services and software are enabled and/or installed.
7.113	The SCDE shall protect all mobile devices with a password or personal identification number (PIN).
7.114	The SCDE shall ensure all mobile devices have timeout/locking features.
7.115	The SCDE shall develop controls for the protection of data storage on mobile devices, including removable media.
7.116	The SCDE shall protect the storage and transmission of information on portable and mobile information devices through scanning the devices for malicious code with virus protection software. Before a mobile device is connected to an SCDE's network, it shall be scanned for viruses. If mobile device is used for transitional storage (e.g., copying data between systems), the data shall be securely deleted from the mobile device immediately upon completion.
7.117	The SCDE shall develop a process for users to notify designated personnel when mobile devices are lost or stolen. The process shall include remote wiping/erasing of mobile devices.
7.118	The physical security of these devices shall be the responsibility of the employee to whom the device has been assigned. Devices shall be kept in the employee's physical presence whenever possible. Whenever a device is being stored, it shall be stored in a secure place, preferably out-of-sight.

7.200 Removable Media Security

The purpose of the removable media security section is to establish security requirements and provide guidance to protect both the physical devices and the information they contain.

Policy ID	Control Description
7.201	The SCDE shall protect information system media until the media is destroyed or sanitized using approved equipment, techniques, and procedures.

Policy ID	Control Description
7.202	For sensitive data, the SCDE shall physically control and securely store digital (e.g., CD, flash drives) and non-digital (e.g., paper) media within secured locations.
7.203	The SCDE shall ensure that only secure portable storage devices (e.g., encrypted flash drives) are utilized as removable media.
7.204	The SCDE shall employ encryption mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.
7.205	The SCDE shall sanitize removable digital and non-digital media prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.

7.300 Portable Computing Devices

The purpose of the Portable Computing Devices security section is to establish security mechanisms to protect both portable computing devices, such as laptops, and the information they contain.

Policy ID	Control Description
7.301	The SCDE shall employ whole disk encryption to protect the confidentiality and integrity of information stored on computing devices, including laptops.
7.302	The SCDE shall configure computing devices operating system (OS) so that only approved services are enabled and/or installed.
7.303	The SCDE shall implement a configuration management process that includes flaw remediation such as installing most current stable security patches, critical security updates, and hot fixes for the relevant OS.
7.304	The SCDE shall implement tools to automatically update virus definition files on laptops and other portable computing devices susceptible to viruses.
7.305	The SCDE shall install firewall software on laptops and implement mechanisms that prevent users from making firewall configuration changes.
7.306	SCDE must ensure asset tags are placed on portable computing devices.
7.307	The SCDE shall disable Peer-to-Peer wireless connections, otherwise known as “Ad-Hoc Connections,” on all portable computing devices, including laptops.

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