STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 8 – Asset 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.

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).

Asset Management Policy Controls

8.100 Asset Identification

The purpose of asset identification is to define the basis for developing an inventory of assets that support the SCDE. Compiling an inventory of assets is important for judging the relative value and importance of agency assets. Based on this information, the SCDE shall provide appropriate levels of protection.

Policy ID	Control Description
8.101	SCDE shall document and maintain inventories of the important assets associated with each information system. Asset inventories shall include a unique system name, a system/business owner, a data classification, and a description of the location of the asset. Examples of assets associated with information systems are as follows: o Information assets: databases and data files, system documentation, user manuals, training material, operational procedures, disaster recovery plans, archived information; o Software assets: application software, system software, development tools and utilities; o Physical assets: physical equipment (e.g., processors, monitors, laptops, portable devices, tablets, smartphones), communication equipment (e.g., routers, servers), magnetic media (e.g., tapes and disks); and o Services: computing and communications services.
8.102	Access to SCDE assets shall be requested via a formal registration process that requires user acknowledgement of all rules and regulations pertinent to the asset.
8.103	SCDE shall periodically revalidate the asset to ensure that it is classified appropriately and that the safeguards remain valid and operative.
8.104	SCDE must classify assets into the data sensitivity classification types in the State of South Carolina Data Classification Schema: Public, Internal, Confidential, and Restricted.
8.105	SCDE shall ensure that each asset is classified based on data classification type and impact level, and the appropriate level of information security safeguards are available and in place.

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