STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 12 – Data Protection and Privacy

Chief Information Security Office

March 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).

Data Protection and Privacy Policy Controls

12.100 Data Classification

The purpose of the data classification section is to define the different categories for SCDE information assets regardless of form. Whether it is electronic, hard copy, or intellectual property.

Policy ID	Control Description
12.101	The SCDE shall categorize data in accordance with applicable federal and state laws, Executive Orders, directive, regulations, and information security guidance. SCDE data shall be classified into one of the following categories: 1. **Public:** Information intended or required for sharing publicly. Examples of public information include information provided on government website and reports meant for public distribution. Unauthorized disclosure, alteration, or destruction of public data would result in minimum to no risk to the State. 2. **Internal Use:** Information that is used in daily operations of the SCDE. Examples of internal use information include the SCDE hierarchy structure, internal procedures, and internal communications. Unauthorized disclosure, alteration, or destruction of internal use data would result in little risk to the State. 3. **Confidential**: Confidential information refers to sensitive information in custody of the SCDE. Examples of confidential information include credit card information, information security plan, system configuration standards, or information exempt from Freedom of Information Act (FOIA). Unauthorized disclosure, alteration, or destruction of confidential data would result in considerable risk to the State. 4. **Restricted**: Restricted information is highly sensitive information in custody or owned by the SCDE and/or data which is protected by federal or state laws and regulations. Examples of restricted information may include, but are not limited to, Federal Tax Information (FTI) and health information protected by the Health Insurance Portability and Accountability Act (HIPAA). Unauthorized disclosure, alteration, or destruction of restricted data shall result in considerable risk to the State, including statutory penalties.
12.102	Users who encounter information that is improperly labeled, according to the data classification descriptions above, shall consult with the owner of the information and/or the SCDE Information Security and/or Data Privacy team(s) to determine the appropriate data classification.

Policy ID	Control Description
12.103	If multiple data fields with different classifications have been combined, the highest classification of information included shall determine the classification of the entire set.

12.200 Data Disposal

The purpose of the data disposal section is to define the controls that shall be followed for disposal of data both in digital and non-digital formats.

Policy ID	Control Description
12.201	The SCDE shall develop a list of approved processes for sanitizing electronic and non-electronic media prior to disposal, release for reuse, and release outside of the SCDE based on applicable regulatory requirements.
12.202	The SCDE shall employ sanitization mechanisms with the strength and integrity commensurate with the security category or classification of the information.
12.203	The SCDE Shall implement controls to track media sanitization and disposal process, wherever compliance requirements dictate such actions must be tracked, documented, and verified. Documentation must provide a record of the media sanitized, when, how media was sanitized, the person who performed the sanitization, and the final disposition of the media. The record of action taken must be maintained in a written or electronic format.
12.204	The SCDE must test media sanitization equipment and procedures at least annually to ensure correct performance.
12.205	The SCDE must ensure that electronic media are securely erased prior to being reassigned, or released for destruction.
12.206	The SCDE must define and implement mechanisms for disposal of digital media and data storage devices contained in equipment to be released outside of the agency.
12.207	The SCDE shall destroy hard copy media containing internal-use, confidential, or restricted information using approved methods prior to disposal.
12.208	The SCDE information security department shall monitor the destruction of hard copy media, as required to ensure and verify compliance with policy.

12.300 Data Protection

The purpose of the encryption section is to define the controls that need to be in-place to protect confidential and restricted data.

Policy ID	Control Description
12.301	SCDE employees shall follow the SCDE's acceptable use policies when transmitting data.
12.302	The SCDE implemented mechanisms to ensure availability of information in the event of the loss of cryptographic keys by users.
12.303	The SCDE shall implement mechanisms to ensure the confidentiality of private keys.
12.304	The SCDE shall develop a mechanism to randomly select a key from the entire key space, using hardware-based randomization.
12.305	The SCDE shall implement appropriate controls to physically and logically safeguard the key-generating equipment from construction through receipt, installation, operation, and removal from service.
12.306	For Restricted or data protected by federal or state laws or regulations: the SCDE shall use Federal Information Processing Standards (FIPS)-140 validated (e.g., Advanced Encryption Standards (AES), Triple Data Encryption Algorithm (TDEA), Diffie-Hellman, RSA, Rivest Cipher 5 (RC5)) technology for encrypting confidential data.
12.307	The SCDE must ensure that sensitive data transmitted by email must be securely encrypted.
12.308	The SCDE must ensure that sensitive information transmitted through a public network must be encrypted prior to transmittal, or be transmitted through an encrypted connection.
12.309	The SCDE must ensure that sensitive information transmitted wirelessly must be encrypted prior to transmittal, or be transmitted through an encrypted connection.

12.400 Privacy

The purpose of the privacy section is to set forth policies the SCDE shall use when information systems or applications will gather Personal Identifiable Information (PII) and/or when webpages are available openly to the public.

Policy ID	Control Description
12.401	The SCDE must designate an individual who has primary responsibility for information privacy decisions.
12.402	Each agency must conduct a Privacy Impact Assessment (PIA) for each information system that will handle Personally Identifiable Information (PII). Each PIA should examine the following privacy issues: • What PII is to be collected. • What is the intended use of the PII. • What PII will be shared, and with whom. • How long the PII will be retained. • What privacy risks are posed by the intended use and sharing of the collected PII. • What privacy risks are posed by unintended disclosure of the collected PII. • What steps are taken to inform users about the PII collected and what mechanisms they can use to control it. • What opportunities individuals have to decline to provide PII. • What steps are taken to minimize the types of PII collected. • What mechanisms are available for data subjects to update or correct their PII. • What opportunities individuals have to remove PII once collected. • How the PII is to be secured. • What processes are established to resolve privacy issues.
12.403	The SCDE must update PIAs when a system change creates changes in privacy risks.
12.404	The SCDE must ensure that PIA documents are reviewed by an agency executive or designee with authority for issues of information privacy.
12.405	Each agency must require each member of agency personnel and third party with access to PII to sign a confidentiality agreement defining responsibilities.
12.406	Each agency must publish a privacy web statement on each agency website used by the public. Each website privacy statement should include, as specifically applicable to the site: • What PII is to be collected. • What is the intended use of the PII. • What PII will be shared, and with whom. • How long the PII will be retained. • What opportunities individuals have to decline to provide PII. • What mechanisms are available for data subjects to update or correct their PII. • What opportunities individuals have to remove PII once collected.

Policy ID	Control Description
	• How the PII is to be secured, in a non-technical summary.. • What processes are established to resolve privacy issues."

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