STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 2 — Access Control

Chief Information Security Office

January 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).

Access Control - Policy Controls

2.100 Access Management

The purpose of the access management section is to establish processes to control access and use of SCDE information resources. Access management incorporates role-based access controls (RBAC), privileged-user access, access definitions, roles, and profiles.

Policy ID	Control Description
2.101	The SCDE shall establish formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.
2.102	The SCDE shall identify account types (e.g., individual, group, system, application, guest/anonymous, and temporary) and establish conditions for group membership.
2.103	The SCDE shall identify authorized users of the information system and specify access rights.
2.104	The SCDE shall establish a process to enforce access requests to be approved by business/data owner (or delegate) prior to provisioning user accounts.
2.105	The SCDE shall authorize and monitor the use of guest/anonymous and temporary accounts and notify relevant personnel (e.g., account managers) when temporary accounts are no longer required.
2.106	The SCDE shall establish a process to notify relevant personnel (e.g., account managers, system administrators) to remove or deactivate access rights when users are terminated, transferred, or access rights requirements change.
2.107	The SCDE shall remove or disable default user accounts, and, if user accounts cannot be removed or disabled, they should be renamed.
2.108	Access shall be granted based upon the principles of need-to-know, least-privilege, and separation of duties. Access not explicitly permitted shall be denied by default.
2.109	Access requests from users shall be recorded and follow the SCDE-established approval process.
2.110	The SCDE shall ensure that user access requests are approved by a business owner (or any other pre-approved role).

Policy ID	Control Description
2.111	Privileged accounts (e.g., system/network administrators having root-level access, database administrators) shall only be allowed after approval by the SCDE information security officer and/or similarly designated role. The approval shall be granted to a limited number of individuals with the requisite skill, experience, business need, and documented reason, based on role requirements.
2.112	The SCDE shall ensure that privileged accounts are controlled, monitored, and can be reported on a periodic basis.
2.113	The SCDE shall regulate information system access and define security requirements for contractors, vendors, and other service providers.
2.114	The SCDE shall establish procedures to administer privileged-user accounts in accordance with a role-based access model.
2.115	The SCDE shall enforce approved authorizations for logical access to information systems.
2.116	The SCDE shall implement encryption as an access control mechanism if required by federal, state, or other laws or regulations.
2.117	For restricted data: SCDE systems shall enforce data-flow controls using security attributes on information, source, and destination objects as a basis for flow-control decisions.
2.118	The SCDE shall implement controls in information systems to enforce separation of duties through assigned access authorizations, including but not limited to: • Audit functions are not performed by security personnel responsible for administering information system access; • Divide critical business and information system management responsibilities; • Divide information system testing and production functions between different individuals or groups; and • Independent entity to conduct information security testing of information systems.

Policy ID	Control Description
2.119	The SCDE shall document and implement separation of duties through assigned information system access authorizations.
2.120	The SCDE shall ensure that only authorized individuals have access to SCDE data/information and that such access is strictly controlled and audited in accordance with the concepts of "need-to-know, least-privilege, and separation of duties".
2.121	The SCDE shall implement processes or mechanisms to: • Disable file system access not explicitly required for system, application, and administrator responsibilities; • Provide minimal physical and system access to the contractors and ensure information security policy adherence by all contractors; • Restrict use of database management to authorized database administrators; • Grant access to authorized users based on their required job duties; and • Disable all system and removable media boot access unless explicitly authorized by the CIO; if authorized, boot access shall be password-protected.
2.122	SCDE systems shall enforce a limit of unsuccessful logon attempts during a SCDE-defined period. The number of logon attempts shall be commensurate with the classification of data hosted, processed, or transferred by the information system.
2.123	The SCDE shall automatically lock user accounts after the maximum logon attempts is reached. The SCDE shall establish an account-lock time period commensurate with the classification of data hosted, processed, or transferred by the information system.
2.124	The SCDE implements warning banners that comply with federal, state, or other laws of regulations associated with the type of data handled by the SCDE (e.g., For FTI IRS Publication 1075 requirements apply).
2.125	The SCDE systems shall time out sessions or require a re-authentication process after (30) minutes of inactivity.

2.200 Network Access Management

The purpose of the network access management section is to establish procedures to control and monitor access and use of the network infrastructure. These are necessary to preserve the integrity, availability, and confidentiality of SCDE information.

Policy ID	Control Description
2.201	The SCDE shall document allowed methods for remote access to the network and information systems.
2.202	The SCDE shall utilize automated mechanisms to enable management to monitor and control remote connections into networks and information systems.
2.203	Virtual Private Network (VPN) or equivalent encryption technology shall be used to establish remote connections with SCDE networks and information systems.
2.204	Remote users shall connect to SCDE information systems only using mechanism protocols approved by the SCDE through a limited number of managed access control points for remote connections.
2.205	For restricted data and/or system administrators: SCDE employees and authorized third parties accessing SCDE information systems remotely shall do so via an approved two-factor authentication (2FA) technology.
2.206	The SCDE shall develop formal procedures for authorized individuals to access its information systems from external systems, such as access allowed from an alternate work site (if required).
2.207	The SCDE establishes usage restrictions, configuration/connection requirements, and implementation guidance for wireless access.
2.208	The SCDE shall only use wireless networking technology that enforces user authentication.
2.209	The SCDE shall authorize wireless access to information systems prior to allowing use of wireless networks.
2.210	The SCDE does not allow wireless access points to be installed independently by users.

Policy ID	Control Description
2.211	If external systems are authorized by the SCDE, the SCDE shall establish terms and conditions for their use, including types of applications that can be accessed from external information systems; security category of information that can be processed, stored, and transmitted; use of VPN and firewall technologies; the use and protection against the vulnerabilities of wireless technologies; physical security maintenance; and the security capabilities of installed software are to be updated.
2.212	The SCDE networks where information deemed critical by the SCDE are stored or processed shall be physically or logically segregated from publicly available networks.
2.213	The SCDE networks and information systems shall not be accessible from pubic networks (e.g., Internet) except under secured and managed interfaces employing boundary protection devices.
2.214	The SCDE limits network access points to a minimum to enable effective monitoring of inbound and outbound communications and network traffic.

9.300 Identity Management

The purpose of the identity management section is to establish a standardized method to create and maintain verifiable user identifiers and enable decisions about the levels of access to be given to each individual and/or groups.

Policy ID	Control Description
2.301	The SCDE shall establish processes to enforce the use of unique system identifiers (User IDs) assigned to each user, including technical support personnel, system operators, network administrators, system programmers, and database administrators.
2.302	The SCDE shall prevent reuse of user identifiers until all previous access authorizations are removed from the system, including all file accesses for that identifier.
2.303	The SCDE shall allow the use of group IDs only where these are necessary for business or operational reasons; group IDs shall be formally approved and documented.
2.304	If the SCDE requires group IDs, it shall require individuals to be authenticated with a unique user account prior to using the group ID (e.g., network authentication prior to use of Group ID).
2.305	The SCDE shall minimize the use of system, application, or service accounts; and it shall document, formally approve, and designate a responsible party of this type of accounts.
2.306	The SCDE security system shall be able to identify and verify the identification and, if deemed necessary by the SCDE, the location of each authorized user.

2.400 Authentication

The purpose of the authentication section is to establish the authentication methods utilized by the SCDE for authenticating, external/remote access connections, VPN access, administrative function access, vendor access, and remote access to sensitive information.

Policy ID	Control Description
2.401	The SCDE shall choose a suitable multifactor authentication technique to substantiate the claimed identity of a user.
2.402	The SCDE shall implement mechanisms to record successful and failed authentication attempts.
2.403	The SCDE shall define a maximum number of invalid logon attempts commensurate to the criticality of network or information systems.
2.404	The SCDE networks and information systems shall disable user access upon reaching the maximum number of invalid access attempts as defined by the SCDE.

2.500 Emergency Access

The purpose of the emergency access section is to establish conditions under which emergency access is granted, outline rules to determine who is eligible to obtain emergency access, and authorize personnel entitled to grant access.

Policy ID	Control Description
2.501	The SCDE shall establish processes and procedures for users to obtain access to required information systems on an emergency basis.
2.502	The emergency procedures shall ensure that: • Only identified and authorized personnel are allowed access to live systems and data; • All emergency actions are documented in detail; and • Emergency action is reported to management and reviewed in an orderly manner. •
2.503	The SCDE will establish a process to automatically terminate emergency accounts within twenty-four (24) hours and temporary accounts with a fixed duration not to exceed three-hundred-sixty-five (365) days.

2.600 Password Policy

The purpose of the password section is to establish uniform and enterprise-wide practices to create, manage, and maintain passwords to ensure expected level of access security. The policy outlines requirements for creation of strong passwords, protection of those passwords, and password change frequency.

Policy ID	Control Description
2.601	The SCDE shall establish a process for password-based authentication to include the following: • Automatically force users (including administrators) to change user account passwords every ninety (90) days, or more often as deemed necessary by the SCDE. • Automatically force system administrators (including database, network, and application administrators) to change user account passwords no less than every sixty (60) days. • Passwords for system accounts to be changed at least every ninety (90) days. • Enforce password minimum lifetime of one (1) day. • Prohibit the use of dictionary names or words as passwords and the use of personal information (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates). • Enforce password complexity consisting of at least eight (8) alphanumeric (i.e., upper- and lowercase letters and numbers) and/or special characters. • Encrypt passwords in storage and during transmission. • Prohibit password reuse for six (6) generations prior to reuse. • For FTI: Change/refresh authenticators every 90 days, at a minimum, for a standard user account; every 60 days, at a minimum, for privileged users. •
2.602	The SCDE users shall not share passwords with others under any circumstance.
2.603	System passwords shall be changed immediately upon termination/resignation of any employee with privileged access.
2.604	The SCDE must prohibit its users from using common words or personal information as passwords (e.g., username, social security number, children's names, pets' names, hobbies, anniversary dates, etc.).

Policy ID	Control Description
2.605	The SCDE shall suspend user accounts after a specified number of days of inactivity.
2.606	The SCDE shall implement a process to change passwords immediately if there is reason to believe a password has been compromised or disclosed to someone other than the authorized user.

2.700 Password Administration

The purpose of the password administration section is to ensure that the allocation of passwords is controlled through a formal management process.

Policy ID	Control Description
2.701	The SCDE users shall sign an acknowledgement to evidence understanding of authentication policies, including the SCDE policy to keep passwords confidential and to keep group passwords solely within the members of the group.
2.702	The SCDE shall establish a process to verify the identity of a user prior to providing a new, replacement, or temporary password.
2.703	The SCDE shall establish a process to uniquely identify and authenticate non-Agency users.
2.704	The SCDE shall establish procedures to manage new or removed privileged-accounts passwords.
2.705	First-time passwords shall be set to a unique value per user and changed immediately after first use.
2.706	The SCDE shall provide temporary passwords to users in a secure manner; the use of third parties or unprotected (i.e., clear text) electronic mail messages shall be prohibited.
2.707	The SCDE shall obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
2.708	The SCDE shall require that employees sign acknowledgement prior to allowing access to network and information systems.
2.709	The SCDE shall not allow default passwords for network and remote applications.

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