STATE OF SOUTH CAROLINA

DEPARTMENT OF EDUCATION

Information Security Policy 11 – Threat and Vulnerability Management

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).

Threat and Vulnerability Management Policy Controls

11.100 Vulnerability Assessment

The purpose of the Vulnerability Assessment policy is to establish controls and processes to help identify vulnerabilities within SCDE technology infrastructure and information system components which could be exploited by attackers to gain unauthorized access, disrupt business operations, and steal or leak sensitive data.

Policy ID	Control Description
11.101	The SCDE shall implement processes to scan for vulnerabilities in information systems and hosted applications at least annually and when new vulnerabilities potentially affecting the information systems/applications are reported.
11.102	The SCDE shall implement a process to control privileged access to vulnerability scanning tools and vulnerability reports.
11.103	The SCDE shall remediate identified vulnerabilities in accordance with the SCDE's assessment of risk.
11.104	The SCDE shall conduct penetration testing exercises on an annual basis, either by use of internal resources or employing an independent third-party penetration team.

11.200 Incident Management

The purpose of the Incident Management policy is to establish controls and processes that will provide the SCDE information system with effective monitoring capability and responsiveness against security threats and incidents. Design and implementation of an incident management framework can secure the information system against known vulnerabilities and threats.

Policy ID	Control Description
11.201	The SCDE shall develop, document, and publish an incident response process that addresses scope, roles, and responsibilities; internal coordination efforts; and compliance.
11.202	The SCDE shall develop and/or hire a third-party vendor to implement an incident response plan to • establish a roadmap for implementing incident response capabilities; • identify and document the requirements of the organization, including mission, size, structure, and functions; • define the types of information security incidents to be reported;

Policy ID	Control Description
	• establish metrics to help ensure incident response capabilities remain effective; and • define resources, such as technology and personnel, required to effectively support incident response capabilities.
11.203	The SCDE must review and update the incident response plan on an annual basis.
11.204	Each agency ensure that information security incident handling processes include preparation, detection and analysis, containment, eradication, and recovery.
11.205	The SCDE must implement dynamic response capabilities/tools such as intrusion detection, intrusion prevention systems, and firewalls, among others, to effectively respond to security incidents
11.206	The SCDE must implement a policy to require personnel to report suspected information security incidents to the incident response team and/or SCDE leadership.
11.207	The SCDE must monitor information systems to detect attacks and/or signs of potential attacks, including unauthorized network local or remote connections.
11.208	The SCDE must ensure that monitoring devices are deployed strategically within information technology environment to collect information security events and associated information.
11.209	The SCDE must ensure the protection of information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion.
11.210	The SCDE must ensure the monitoring of inbound and outbound communications traffic from sensitive information systems for unusual or unauthorized activities or conditions.
11.211	The SCDE must ensure that information system monitoring activity is appropriately adjusted for new and increased sources of risk.
11.212	The SCDE must provide incident response training within one (1) month of personnel assuming incident response roles or responsibilities.
11.213	The SCDE must provide training to incident response personnel upon significant changes to information systems and/or changes to the incident response plan.

Policy ID	Control Description
11.214	The SCDE must establish a formal process to test incident response capabilities on a yearly basis to determine the incident response effectiveness and adequacy.
11.215	The SCDE must document the incident response test results and update incident response processes as applicable.
11.216	The SCDE must ensure malicious code protection mechanisms are employed for information systems, to detect and eradicate malicious code.
11.217	The SCDE must ensure malicious code protection mechanisms are updated whenever new releases are available.
11.218	The SCDE must ensure malicious code protection mechanisms are configured to perform periodic scans at defined time intervals.
11.219	The SCDE must ensure malicious code protection mechanisms are configured to send an alert to information appropriate personnel, to initiate appropriate actions in response to malicious code detection.

11.300 Patch Management

The purpose of the Patch Management policy is to identify controls and processes that will provide appropriate protection against threats that could adversely affect the security of the information system or data entrusted on the information system. Effective implementation of these controls will create a consistently configured environment that is secure against known vulnerabilities in operating system and application software.

Policy ID	Control Description
11.301	The SCDE shall develop and implement a process to identify, report, and correct information system flaws.
11.302	The SCDE shall establish a formal process to test software and firmware updates related to flaw remediation for effectiveness and identification of potential impact prior to implementation.
11.303	The SCDE shall install latest stable versions of applicable security software and firmware updates.
11.304	The SCDE shall establish a patch cycle that guides the normal application of patches and updates to systems.

Policy ID	Control Description
11.305	The SCDE shall establish a process of patch testing to verify the source and integrity of the patch and ensure testing in a production-mirrored environment for a smooth and predictable patch roll out.

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