SOUTH CAROLINA
DEPARTMENT OF EDUCATION

SAFE K-12 Charter: An Information Security Support Program

March 2026

Ellen E. Weaver
State Superintendent of Education

Contents

SAFE K-12 Information Security Program Charter

Purpose

South Carolina education organizations are obligated to protect the sensitive data and resources used in performing their mission of educating children in the State. This document describes the South Carolina Department of Education (SCDE) SAFE K-12 Information Security Program for constituent K-12 schools and school districts within the State of South Carolina. This program is a set of policies, procedures, and responsibilities for the protection of institutional and citizen data.

The SAFE K-12 Information Security Program supports participating organizations in ensuring the confidentiality of K-12 records and related computing resources, protecting against anticipated threats and hazards to the integrity of K-12 data and prevent unauthorized access to information or computer resources associated with protected K-12 data.

Authority

South Carolina Code Section 59-1-490(G) provides, "[e]ach school district in this State shall adopt, maintain, and comply with a locally adopted student records governance and use policy. These policies and their implementation shall be monitored by the State Department of Education in a manner prescribed by the department through policy. "

SAFE K-12 Program is the way the SCDE ensures adequate statewide compliance with student records governance and use policies as well as provide guidance and resources to organizations to meet their records governance and use policy.

Scope of SAFE K-12

Covered data includes any data owned, managed, or provided by SC K-12 schools that comprise student records, either directly or indirectly or systems which store, process, or transmit student records. The program will be governed by SCDE as well as any applicable laws and standards of the State of South Carolina and the United States Federal government.

Service Model

The SAFE K-12 Program follows both the centralized and distributed models of IT service delivery. Centralized elements—managed by SCDE—include a set of common controls that describe functions such as security policy implementation, program awareness and training, and purchasing vehicles. Distributed elements include use of common controls, controls delivered as self-service or vendor-performed service, and any controls or safeguards necessary in the individual needs of the organizations for the conducting their business. SCDE is responsible for leadership of the centralized elements and coordination of the distributed elements.

Roles and Responsibilities

SCDE Responsibilities

The SAFE K-12 Information Security Program is governed by SCDE for security requirements and overall program monitoring and adjustments. SCDE may delegate security control capabilities and support structures to other entities, but SCDE reserves the right to monitor. SCDE is responsible for providing strategic oversight of the Information Security Program and maintaining the Information Security Program Charter.

The SCDE Chief Information Security Officer (CISO) or their designee (Program Officer) is responsible for coordinating and overseeing the Information Security Program. The Program Officer will serve as the primary point of contact for Districts for this Information Security Program. The Program Officer may designate other representatives to oversee and coordinate portions of the program. Any questions regarding the implementation of this program or the interpretation of this document should be directed to the Program Officer.

At a minimum, the SCDE will perform the following:

- The Program Officer will provide leadership for the Information Security Office that is tasked with execution of the SAFE K-12 Program.
- The Program Officer will consult with responsible offices of each participating organization to identify the security risks and specific needs of each of the units and areas of the participating organization with access to covered data.
- The Program Officer may periodically conduct security assessments of Districts to test safeguards and ensure compliance (e.g., review of security tool usage to ensure vulnerability scans are occurring at the prescribed intervals.)
- The Program Officer will create and distribute a model Incident Response Policy for addressing information security incidents for adoption or adaptation by the participating organizations.
- The Program Officer will, in consultation with the participating organization, verify that existing policies, standards and guidelines that provide for the security of covered data are reviewed and adequate. In some cases, the Program Officer may require external vendor partners with substantial access to covered data to further develop and implement comprehensive security plans specific to those units and to provide copies of the plan documents.
- The Program Officer may make recommendations for revisions to policy, or the development of new policy, as appropriate.

- The Program Officer will work with responsible parties to ensure that the participating organizations' training and education plans are developed and delivered for all employees with access to covered data.

District Responsibilities

At a minimum, school or district participants in SAFE K-12 will perform the following:

- All participating organizations will designate a representative for their Information Security Program who will serve as the primary point of contact for all SCDE Information Security Program requirements within their area of responsibility.

- All participating organizations must plan for adequate funding and resources to implement information security program requirements as directed by the SAFE K-12 Program within appropriate timeframes or address needs with SCDE prior to compliance timelines. SCDE recognizes the substantial resource commitment that any information security program requires and understands that each participating organization has challenges outside of information security.

- All participating organizations must enforce SAFE K-12 standards and requirements on any partners, vendors, or tools used in their environment or document deviations with approval from SCDE.

Considerations

- While no information security program can eliminate all risk to system and data, the SAFE K-12 program is structured to prioritize organizational resources on efforts that will reduce risk to as little as possible while still allowing flexibility for participants to accept risks based on their business needs.

- The final security responsibility of the covered data rests with the participating organization unless specifically agreed upon and documented by both SCDE and the participating organization. While compliance with the cybersecurity best practices of the program is considered mandatory, should a participating organization choose not to meet the SAFE K-12 requirements, these instances must be agreed upon by SCDE and the participating organization prior to implementation timeframes. Risk-based decisions on implementation strength or methods will be the responsibility of the participating organization and is expected to be documented and justifiable.

- When required by the cyclical review components of the SAFE K-12, participating organizations must support risk assessments and ongoing monitoring of information security posture as directed by the SCDE. Any deviations from risk assessments and/or monitoring must be agreed upon by the SCDE and the participating organization prior to implementation.

- The capabilities and tools provided under the SAFE K-12 program will have different billing, usage, and operating models available to the schools or districts. Each school or district must enter into an agreement with SCDE on how the capability or tool will be used prior to implementing or using any tool. SCDE reserves the right to ensure the participating organization honor any commitments or obligations.

- Any deviation from the standard provisions of the Information Security Program will require the approval of the SCDE Office of General Counsel and the SAFE K-12 Program Officer. These standards shall apply to all contracts entered into with third-party service providers.

- By participating in SAFE K-12 and using the resources and contract methods involved in the program, organizations are required to provide accurate and current status and fully utilize the tools according to minimum standards established by the program. Should an organization not use the methods or tools properly or choose not to participate appropriately, the Information Security and Risk Oversight Group reserves the right to remove the organization from the SAFE K-12 program once all contracts have expired. Should an extreme case of misuse arise, SCDE may terminate any standing agreements immediately via their General Counsel direction.

Adjustments and Maintenance of the Information Security Program.

SCDE is responsible for evaluating and specifying adjustments to the District Information Security Program based on the risk identification and assessment activities undertaken pursuant to this program, as well as any material changes to the Institution's operations or other circumstances that may have a material impact on this program.

Exceptions to the Program

Exceptions or waivers to this Program or its subsequent practices, procedures or standards must be authorized by SCDE. Exceptions or waivers to any practices, controls, or standards will be properly documented and reviewed on a periodic basis.

Privacy Considerations

While there are many areas of overlap between security and privacy the information security program is not designed to address privacy concerns of covered data, which will be covered by each organization’s Privacy Policies. However, the information security office will take all measures possible to address proper handling of data that is required to secure the organization and will only use such data for the intended purposes outlined in this charter.

Vision

The SCDE recognizes that good faith partnerships throughout the State are integral in ensuring the security of information systems and student records. The SCDE appreciates the dialogue with districts and schools that will facilitate continued improvements for the

benefit of students, families, and staff. In fulfilling its statutory responsibility to monitor data governance policies and implementation, the SCDE intends to create a system and supports that positions districts for success.

Appendix A – Information Security Framework

The SCDE K-12 Information Security Framework is intended to be a common lexicon used by Districts to establish a minimum-security baseline for all participating organizations while also providing resource and cost optimization amongst the organization. This framework is based on the CIS Critical Security Controls and associated policies, guidance and documents but tailored for the State of South Carolina.

If using an alternative framework to the CIS CSC, the District can use any terminology or structure that meets their needs but will be required to work with SCDE on documenting and demonstrating compliance with the Information Security Program.

SCDE will provide security tools or capability options, security services options, and/or guidance around the high-level CIS Critical Security Controls. The CIS Critical Security Controls will address security activities in the following areas[1]:

Inventory and Control of Enterprise Assets

Actively manage (inventory, track, and correct) all enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/Internet of Things (IoT) devices; and servers) connected to the infrastructure physically, virtually, remotely, and those within cloud environments, to accurately know the totality of assets that need to be monitored and protected within the enterprise. This will also
support identifying unauthorized and unmanaged assets to remove or remediate.

Inventory and Control of Software Assets

Actively manage (inventory, track, and correct) all software (operating systems and applications) on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

Data Protection

Develop processes and technical controls to identify, classify, securely handle, retain, and dispose of data.

Secure Configuration of Enterprise Assets and Software

Establish and maintain the secure configuration of enterprise assets (end-user devices, including portable and mobile; network devices; non-computing/IoT devices; and servers) and software (operating systems and applications).

Account Management

Use processes and tools to assign and manage authorization to credentials for user accounts, including administrator accounts, as well as service accounts, to enterprise assets and software.

Access Control Management

Use processes and tools to create, assign, manage, and revoke access credentials and privileges for user, administrator, and service accounts for enterprise assets and software.

Continuous Vulnerability Management

Develop a plan to continuously assess and track vulnerabilities on all enterprise assets within the enterprise's infrastructure, in order to remediate, and minimize, the window of opportunity for attackers. Monitor public and private industry sources for new threat and vulnerability information.

Audit Log Management

Collect, alert, review, and retain audit logs of events that could help detect, understand, or recover from an attack.

Email and Web Browser Protections

Improve protections and detections of threats from email and web vectors, as these are opportunities for attackers to manipulate human behavior through direct engagement.

Malware Defenses

Prevent or control the installation, spread, and execution of malicious applications, code, or scripts on enterprise assets.

Data Recovery

Establish and maintain data recovery practices sufficient to restore in-scope enterprise assets to a pre-incident and trusted state.

Network Infrastructure Management

Establish, implement, and actively manage (track, report,
correct) network devices, to prevent attackers from exploiting vulnerable network services and access points.

Network Monitoring and Defense

Operate processes and tooling to establish and maintain comprehensive network monitoring and defense against security threats across the enterprise's network infrastructure and user base.

Security Awareness and Skills Training

Establish and maintain a security awareness program to influence behavior among the workforce to be security conscious and properly skilled to reduce cybersecurity risks to the enterprise.

Service Provider Management

Develop a process to evaluate service providers who hold sensitive data or are responsible for an enterprise's critical IT platforms or processes, to ensure these providers are protecting those platforms and data appropriately.

Application Software Security

Manage the security life cycle of in-house developed, hosted, or acquired software to prevent, detect, and remediate security weaknesses before they can impact the enterprise.

Incident Response Management

Establish a program to develop and maintain an incident response capability (e.g., policies, plans, procedures, defined roles, training, and communications) to prepare, detect, and quickly respond to an attack.

Penetration Testing

Test the effectiveness and resiliency of enterprise assets through identifying and exploiting weaknesses in controls (people, processes, and technology) and simulating the objectives and actions of an attacker.