SOUTH CAROLINA
DEPARTMENT OF EDUCATION

SAFE K-12:
South Carolina's Assurance Framework for Education Cybersecurity

Helping school districts plan and implement cybersecurity effectively and efficiently.

Updated August 2025

Ellen E. Weaver
South Carolina Department of Education

Contents

Executive Summary 1

What is SAFE K-12? 1

What SAFE K-12 Provides 1

How it Works..1

Cost & Savings 2

Example Savings: 2

Budget Planning Formula:..2

“Pay Now, True-Up Later” Approach: 2

Roles & Responsibilities 2

1. Program Overview 3

2. CIS Cybersecurity Framework..3

Why CIS Critical Security Controls (v8)?..3

Options for Districts 4

3. Program Structure, Roles, and Responsibilities 4

SCDE Oversight and Support Responsibilities 4

District Responsibilities 2

Flexible Service Models 2

4. Implementation 2

Phase 1: Foundation Building (Year 1) 2

Phase 2: Expanded Protections (Year 2) 3

Phase 3: Maturity & Sustainability (Year 3)..3

5. Cost Model and District Budget Planning Framework..3

Shared Cost Approach 3

Pricing Model for Districts..4

How it Works:..4

District Budgeting:..4

Appendix: SAFE K-12 Tools & Service Offerings 6

Executive Summary

What is SAFE K-12?

SAFE K-12 is a **statewide cybersecurity support program** led by the South Carolina Department of Education (SCDE) to help public school districts implement foundational cybersecurity protections, effectively, affordably, and with local control.

The program is grounded in the **CIS Critical Security Controls (v8)** and focuses on Implementation Group 1 (IG1) controls, essential safeguards every district must implement regardless of size.

What SAFE K-12 Provides

SAFE K-12 empowers every district, regardless of size or technical capacity, to take meaningful steps to protect data and operations.

What SAFE K-12 Provides	What Districts Receive
Statewide Cybersecurity Framework	Standardized cybersecurity foundation using CIS Controls (v8 IG1), with SCDE/DDGG oversight.
Expert Support & Shared Resources	Guidance, templates, training, and assessment tools to support local implementation.
Affordable, Scalable Solutions	Access to high-quality cybersecurity services at discounted state-negotiated pricing.
Ongoing Monitoring & Compliance Support	Assistance with audits, risk assessments, and meeting S.C. Code §59-1-490(G) requirements.

How it Works

Districts retain flexibility in how they engage with the program, while benefiting from core supports. SAFE K-12 offers a menu of vetted services (such as endpoint security, data backup, phishing simulations, and vulnerability management) negotiated by SCDE at discounted rates to reduce costs. Districts can:

1. Use their own systems and tools;
2. Adopt all tools from the SAFE K-12 vendor catalog;
3. Combine both in a tailored hybrid approach.

Regardless of participation in shared services, all districts must meet minimum cybersecurity requirements under S.C. Code §59-1-490(G).

Implementation Phase	Focus	Year
Phase 1: Foundation	Launch assessments, tools, governance, and MOUs	2025–26
Phase 2: Expansion	Broaden implementation, expand services and training	2026–27
Phase 3: Maturity	Sustain IG1 controls, audit and refine practices	2027–28

Cost & Savings

SAFE K-12 uses a tiered pricing model that rewards statewide participation with lower costs. SCDE also anticipates covering one-time costs such as asset discovery and deployment services to help districts onboard effectively.

Example Savings:

Many districts currently pay up to $15 per endpoint for a specific subset of cybersecurity services. Through SAFE K-12, those same services are available at $2.95 per endpoint.

- A district with 15,000 students (approx. 45,000 devices) could save **$542,000 per year**.
- If adopted statewide, **total savings could exceed $10 million annually**, depending on participation levels.

Budget Planning Formula:

To help districts plan, SCDE recommends a simple budgeting model:

> **$45,000 Base Cost** + **$15 per student above 3,000 enrollment**

For example, a district with 20,000 students would annually plan for approximately $300,000.

"Pay Now, True-Up Later" Approach:

Because statewide participation will influence final pricing, districts will initially pay an estimated rate. Once all commitments are finalized, SCDE will calculate the final cost and issue credits or reimbursements if actual pricing is lower.

Roles & Responsibilities

Districts	SCDE
Designate a cybersecurity lead	Provide statewide tools, templates, and vendor-negotiated services
Meet CIS IG1 controls (minimum requirement)	Define and oversee cybersecurity standards with DDGG
Report progress and participate in audits	Monitor implementation and support compliance with state law
Budget and plan for implementation	Offset one-time onboarding costs (e.g., asset discovery, deployment)

1. Program Overview

The South Carolina Assurance Framework for Education Cybersecurity (SAFE K-12) is a statewide initiative led by the South Carolina Department of Education (SCDE) to strengthen cybersecurity across all public-school districts. The program was created in response to the growing threat of cyberattacks on K–12 institutions and the increasing complexity of securing student and institutional data.

1. **Establish a Statewide Cybersecurity Framework**: SAFE K-12 provides a standardized information security program for all districts, setting a minimum cybersecurity baseline while allowing flexibility for local implementation. It is based on the nationally recognized CIS Critical Security Controls and is overseen by SCDE's Director of Information Security and the District Data Governance Group (DDGG).
2. **Deliver Expert Support**: The program offers expert guidance, templates, vetted resources, and governance to strengthen cybersecurity statewide. It also trains local staff to identify risks and implement security controls. Participants gain access to shared tools, technical guidance, policy templates, training, and monitoring support.
3. **Provide Affordable Solutions**: SAFE K-12 delivers technical and procedural security solutions at state-level pricing, enabling districts to access high-quality cybersecurity services at reduced costs through statewide contracts.
4. **Enable Statewide Monitoring**: The program monitors and assesses cybersecurity across districts to address common challenges efficiently and ensures compliance with S.C. Code Section 59-1-490(G)

SAFE K-12 empowers every district, regardless of size or technical capacity, to take meaningful steps to protect data and operations, contributing to the overall resilience of South Carolina's K–12 education system. Districts may choose to opt out of SAFE K-12, but they must still meet the minimum cybersecurity framework standards.

2. CIS Cybersecurity Framework

K-12 schools face rapidly growing and complex cybersecurity challenges, from safeguarding student records to managing third-party tools, often without dedicated staff or resources. The SAFE K-12 program addresses this need through a structured, flexible framework tailored to school environments.

Why CIS Critical Security Controls (v8)?

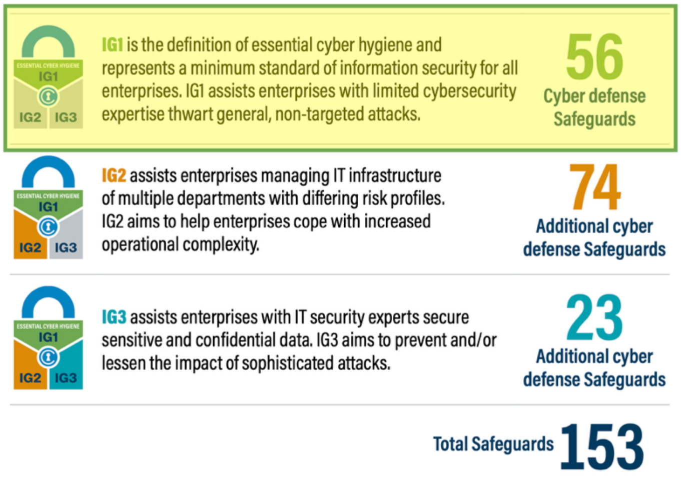
To guide implementation statewide, SCDE selected the Center for Internet Security (CIS) Critical Security Controls (v8) after evaluating multiple national cybersecurity standards. While other frameworks exist—including NIST SP 800-53, ISO/IEC 27001, and CISA's Cybersecurity Performance Goals—CIS was chosen for its balance of rigor, clarity, and usability in school environments. It offers:

- A prioritized roadmap based on real-world threats,
- Outcome-driven safeguards grouped by implementation level, and
- Practical tools and guidance for organizations of all sizes.

The CIS framework includes 153 safeguards, organized into three tiers known as Implementation Groups (IGs) shown in Table 1. **SAFE K-12 prioritizes IG1**, the most critical and achievable 56 safeguards for schools. These controls span several core areas, including:

- **Asset Management**: tracking devices and software,
- **Data Protection & Recovery**: safeguarding sensitive information and ensuring backup integrity,
- **Access Control**: managing user accounts and permissions,
- **Vulnerability Management**: keeping systems patched and protected, and
- **Incident Response & Planning**: preparing for and responding to cyber threats.

Table 1: CIS Framework Implementation Groups



IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.	**56** Cyber defense Safeguards
IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.	**74** Additional cyber defense Safeguards
IG3 assists enterprises with IT security experts secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.	**23** Additional cyber defense Safeguards
Total Safeguards	**153**

Options for Districts

While CIS is the foundation of SAFE K-12, the framework is not mandatory. Districts may use their own cybersecurity programs if they meet or exceed the minimum requirements defined in by the CIS IG1 controls.

SCDE is committed to making implementation as efficient, practical, and locally manageable as possible. The program will be continuously reviewed and refined to reflect evolving threats, statewide feedback, and opportunities for improvement.

3. Program Structure, Roles, and Responsibilities

The SAFE K-12 program is structured to balance **state-level coordination** with **district-level flexibility**. While the South Carolina Department of Education (SCDE) sets the statewide framework and minimum standards, each district determines how best to meet those standards based on its local context.

SCDE Oversight and Support Responsibilities

Led by SCDE's Information Security program, SAFE K-12 will be governed by the District Data Governance Group (DDGG) and guided by a formal program charter. SCDE is responsible for:

- Defining minimum cybersecurity requirements (through CIS Critical Security Controls v8),
- Monitoring compliance in alignment with S.C. Code Section 59-1-490(G),
- Providing statewide tools and services to districts (e.g., vulnerability scans, templates, training),
- Offering unified support, guidance, and risk assessments, and

- Conducting regular audits and compliance reviews.

SCDE is focused on outcomes, not specific technologies. Districts have flexibility in how they meet the standards, but results must align with the goals of SAFE K-12.

District Responsibilities

All school districts, whether participating in the program directly or operating independently, must:

- Designate a local information security lead,
- Implement safeguards that meet or exceed SCDE's minimum requirements,
- Report on cybersecurity status and compliance, and
- Cooperate with assessments and audits.
- Budget appropriately for cybersecurity

Districts may opt out of services offered through SAFE K-12 if they already operate an equivalent or stronger cybersecurity program. However, opting out does not exempt a district from compliance. Districts must still provide documentation and participate in SCDE-led monitoring efforts.

Flexible Service Models

SAFE K-12 is designed to accommodate a range of implementation approaches, including:

1. **Fully District-Managed:** The district independently selects and manages all cybersecurity tools, services, and vendors, while ensuring compliance with SAFE K-12 requirements.
2. **Full Adoption of State-Negotiated Services:** The district chooses to implement all available services and tools from the state-negotiated catalog.
3. **Hybrid Approach:** The district used select offerings from the state catalog to supplement its own tools and services, creating a tailored approach that fits its needs and meets required safeguards.

This flexibility ensures that all districts, regardless of size or resources, have viable paths to cybersecurity readiness, supported by tools and services negotiated at the state to reduce costs and increase access.

4. Implementation

SAFE K-12 will be rolled out in phases over three years, guided by ongoing district input, legal coordination, and evolving cybersecurity needs. The plan prioritizes foundational protections first, while building capacity and infrastructure for long-term resilience.

Phase 1: Foundation Building (Year 1)

1. **District Cybersecurity Survey & Readiness Assessment**
   SCDE will launch a statewide survey to assess each district's cybersecurity posture, identify gaps, and determine what support and services are needed to meet CIS IG1 controls.

2. **Charter, Auditing & Governance**
   In collaboration with the District Data Governance Group (DDGG), SCDE will finalize the SAFE K-12 charter, including audit procedures, risk assessment protocols, and compliance benchmarks.
3. **Memorandum of Understanding**
   In coordination with DDGG, SCDE's Office of General Counsel will draft **MOUs** outlining both SCDE and district participation and coordination responsibilities.
4. **Launch of State-Negotiated Vendor Tools and Services**
   Districts will have the option to purchase state-negotiated vendor services aligned with the Year 1 CIS IG1 controls, as outlined in the Appendix. Multiple vendors will be available, allowing districts to choose the tools and providers that best meet their needs.

Phase 2: Expanded Protections (Year 2)

In Year 2, SCDE will continue deploying IG1 controls with a focus on broader adoption and deeper integration across districts. This phase includes expanded consultative support, increased availability of implementation tools, and continued rollout of services like monitoring assistance, training, and policy guidance. Districts will refine their use of IG1 controls based on lessons learned in Year 1.

Phase 3: Maturity & Sustainability (Year 3)

In Year 3, the focus will shift to sustaining and optimizing IG1 control implementation. Districts will strengthen documentation, maintain ongoing staff training, and institutionalize cybersecurity practices. SCDE will establish a regular review cycle for audits, feedback, and program updates to support continuous improvement and long-term resilience. A CIS Control Implementation Matrix will accompany the full program guide, mapping available services to IG1 controls across all three years.

5. Cost Model and District Budget Planning Framework

Shared Cost Approach

SAFE K-12 costs will vary significantly by district, depending on:

- Existing cybersecurity capacity
- Level of support needed
- Services selected from the state-negotiated vendor catalog

Some districts may continue using their existing solutions, while others may choose to adopt many or all of the tools offered through the program.

To make the program affordable and scalable:

- The SCDE will subsidize a portion of the program's overall cost.
- Districts will cover the remainder based on enrollment, needs, and services selected.

In addition to ongoing service subsidies, SCDE anticipates covering certain one-time implementation costs, such as asset discovery and deployment support, to reduce barriers to participation and ensure strong initial execution. These upfront services will help districts adopt protections more efficiently and may significantly reduce long-term costs.

Statewide negotiated pricing will also deliver substantial savings to districts. By aggregating demand across the state, SCDE has secured pricing that is significantly lower than what most districts—especially smaller ones—could negotiate independently. Final savings will depend on the number of participating districts, but all districts benefit from the shared cost model and economies of scale. At full implementation, potential savings statewide could exceed $8M annually across all cybersecurity services.

Table 2 illustrates potential savings for districts of different sizes for two sample cybersecurity services.

*Table 2: SAFE K-12 Cost Savings for Sample Cybersecurity Services**

	Integrated Cybersecurity Platform			Security Awareness Training		
District Size	**Individually**	**State Pricing**	**Savings**	**Individually**	**State Pricing**	**Savings**
Small (3,000)	$166,320	$26,550	**$139,770**	$12,000	$1,500	**$10,500**
Medium (10,000)	$285,900	$88,500	**$197,400**	$17,500	$5,000	**$12,500**
Large (30,000)	$525,600	$265,500	**$260,100**	$45,000	$15,000	**$30,000**

*Estimates to be finalized once vendor contracts and district selections are confirmed.

Pricing Model for Districts

To ensure districts benefit from statewide volume pricing, regardless of when they commit, SCDE is implementing a **"pay-now, true-up-later" model**.

How it Works:

1. Districts pay the posted tiered rate based on projected statewide participation.
2. Final license counts are calculated once all participating districts commit.
3. If final pricing is lower, districts will receive reimbursement or credit for the difference.

This approach protects early adopters from overpaying and ensures all districts share in the savings from bulk purchasing, even if they commit before final participation numbers are known.

District Budgeting:

To support planning, SCDE recommends the following baseline budget estimate for districts:

> **$45,000 Base Cost** + **$15 per student above 3,000 enrollment** (Head count)

*Table 3: Sample SAFE K-12 District Budget Estimates**

Example	Student Count	Estimated Budget
Small District	1,000 students	$45,000
Mid-size District	20,000 students	$300,000
Large District	60,000 students	$900,000

*These are general planning figures. Actual district costs will vary based on tool selection and service needs.

The SCDE is committed to making cybersecurity costs predictable, scalable, and tied to real service needs. The SCDE will provide regular updates on:

- Finalized vendor pricing,
- District uptake and projected reimbursements, and
- Integration into annual planning cycles.

6. State-Level Resources and Support

To ensure successful implementation and long-term sustainability of SAFE K-12, the South Carolina Department of Education (SCDE) will provide centralized leadership, technical infrastructure, and ongoing operational support. Key state-level resources include:

- **Program Governance**: Led by SCDE's Information Security team in collaboration with the District Data Governance Group (DDGG), responsible for establishing the program charter, audit protocols, and compliance benchmarks.
- **Implementation, Training & Onboarding**: A dedicated Service Delivery Manager will coordinate onboarding, training, and district engagement. SCDE will also provide policy templates, professional development, and on-site support to build local capacity.
- **Technical Services**: SCDE will manage state-negotiated tools for asset discovery, vulnerability management, and secure configurations. Centralized deployment engineers and managed service providers will support implementation and integration.
- **Monitoring & Compliance**: SCDE will conduct regular audits, risk assessments, and compliance tracking in alignment with S.C. Code §59-1-490(G), ensuring districts meet the minimum cybersecurity standards.

Appendix: SAFE K-12 Tools & Service Offerings

Service	Freq.	Services Provided (IG1 Controls Addressed)	Total Controls	Sizing Tiers	Count Type	Price Per Unit	Year Avail.
Tenable One			**22**				**25-26**
Pre-deployment	One-time	Asset Discovery: Prerequisite to deploy Tenable One for Asset & Software Inventory		<5,000	District Student Count	$15,000	
				5,001-10,000		$18,000	
				10,001-20,000		$24,000	
				20,001-35,000		$33,000	
				>35,000		$57,000	
Tenable One Subscription	Ongoing	Asset & Software Inventory (1.1–1.2, 2.1–2.3)		<9,000	Endpoints*	~$18.48	
		Secure Configurations (4.1–4.7)		9,001-30,000		~$9.53	
		Account & Access Management (5.1, 6.3–6.5)		30,001-600,000		~$5.84	
		Vulnerability Management (7.1–7.4)		>600,000		$2.95	
		Email & Web Browser Protections (9.1)					
		Network Infrastructure Management (12.1)					
Deployment	One-time			<5,000	District Student Count	$10,000	
				5,001-10,000		$12,500	
				10,001-20,000		$17,000	
				20,001-35,000		$25,000	
				>35,000		$40,000	
Managed Services	Ongoing	Exposure Management (optional)			District	$10,000	
Training	One-time	On-Site Onboarding & Training			Session	$15,500	
State-level Support	Ongoing	Service Delivery Manager			State	$16,500/Month	
Tenable Vulnerability Management			**4**				**25-26**
Tenable Vulnerability Management Subscription	Ongoing	Vulnerability Management (7.1–7.4)		<1,000	Endpoints	$13.78	
				1,001-5,000		$6.70	
				5,001-10,000		$3.94	
				10,001-20,000		$2.16	
				20,001-50,000		$1.48	
				50,001-100,000		$1.28	
				>100,000		$1.19	

Service	Freq.	Services Provided (IG1 Controls Addressed)	Total Controls	Sizing Tiers	Count Type	Price Per Unit	Year Avail.
Managed Services	Ongoing	Vulnerability Management Service		<1,000	Endpoints	$7.31	
				1,001-5,000		$3.27	
				5,001-10,000		$2.91	
				10,001-20,000		$2.68	
				20,001-50,000		$1.77	
				50,001-100,000		$1.30	
				>100,000		$0.87	
KnowBe4			**8**				**25-26**
KnowBe4 Diamond Level Subscription (Staff)	Ongoing	Security Awareness & Training (14.1–14.8)		<3000	Staff Users	$18.36	
				3,001-10,000		$8.64	
				10,001-30,000		$7.02	
				30,001-117,000		$3.78	
				>117,000		$2.40	
CyberNut			**8**				**25-26**
CyberNut Subscription (Staff)	Ongoing	Security Awareness & Training (14.1–14.8)		<3000	Staff Users	$12.00	
				3,001-10,000		$9.00	
				10,001-30,000		$4.80	
				30,001-125,000		$4.00	
CyberNut Subscription (Student)	Ongoing	Security Awareness & Training (14.1–14.8)		<3000	Student Users	$4.00	
				3001-10,000		$1.75	
				10,001-30,000		$1.50	
				30,001-125,000		$1.00	
				>125,000		$0.50	
Fortinet			**32**				**25-26**
EPP/ATP Cloud	Ongoing	Asset & Software Inventory (1.1–1.2, 2.1–2.2) Data Protection (3.3, 3.6) Secure Configurations (4.1–4.7) Account & Access Management (5.1, 6.3–6.5) Vulnerability Management (7.1–7.4) Audit Log Management (8.1–8.3) Email & Web Browser Protection (9.1–9.2, 10.1–10.3) Network Infrastructure Management (12.1) Penetration Testing & Remediation (17.1–17.2)			Users	$22.10 (+$9.35 Chromebook Add-on)	

Service	Freq.	Services Provided (IG1 Controls Addressed)	Total Controls	Sizing Tiers	Count Type	Price Per Unit	Year Avail.
Firewalls, UTM and SOCaaS		*Fortinet requires purchase of 2 firewalls and licenses		3,000 10,000 30,000	District (based on size)	**$34,204 $48,201 $72,191	
Deployment & Training	One-time	Engineer resident to work with districts for deployment and training			State	$414,000	
State-Level Support Services							**25-26**
Program Governance		Charter, audit protocols, compliance benchmarks, DDGG oversight		<10	Districts Participating	3–4 FTEs [$400,000–$600,000]	
Implementation, Training & Onboarding		Implementation management, onboarding, training, service coordination		10-40		5–7 FTEs [$500,000–$1,000,000]	
Technical Services		Service engineers, help desk, tool management		>50		8–10 FTEs [$900,000–$1,500,000]	
Monitoring and Compliance		Audits, risk assessments, compliance tracking, reporting systems					
Other Services			**14**				**26-27**
		Data Backup & Recovery (11.1–11.4)					
		Data Protection & Lifecycle Management (3.1–3.2, 3.4–3.5)					
		Account Control & Credential Management (5.2–5.4)					
		Access Authorization & Permission Review (6.1–6.2)					
		Service Provider Management (15.1)					