

MEMORANDUM

TO: District Superintendents
District Chief Information Officers
District Chief Information Security Officers

FROM: Dan Ralyea
Chief Information Officer, Information Technology

DATE: March 3, 2026

RE: SAFE K-12 Program Update and Planning for 2026-27

State law requires every South Carolina school district to meet **minimum cybersecurity standards** to protect student data, instructional continuity, and district operations. **Compliance is not optional**—and failure to implement required controls places districts at operational, financial, and legal risk. Districts should be aware that they **may need to allocate budget** to meet these mandated security requirements.

Last August, SCDE introduced you to SAFE K-12, South Carolina’s statewide cybersecurity support program designed to help districts meet these requirements. We encourage you to revisit the [August memo](#) and review the [full program overview](#).

SAFE K-12 equips districts with practical, affordable, and locally controlled methods for implementing essential safeguards. The program is built on nationally recognized cybersecurity standards that every district must meet to protect its systems, its employees, and its students.

Under state law and the SAFE K-12 framework, districts are responsible for implementing the safeguards, designating a cybersecurity lead, participating fully in program assessments, and planning appropriate budgets to support ongoing cybersecurity needs. SCDE provides the tools, guidance, frameworks, training, and access to discounted statewide cybersecurity services, but successful implementation depends on strong district leadership and clear prioritization at the superintendent level.

Progress Since August

Since launching the program, SAFE K-12 has delivered the foundational supports districts need to move into active implementation:

- **Supported District Cybersecurity Assessment:** Developed guidance for districts to complete the CIS Controls Self-Assessment Tool (CSAT).
- **Established Governance and Support Structure:** Created the [SAFE K-12 Program Charter](#) and staffed a centralized SCDE team dedicated to supporting district cybersecurity efforts.
- **Built Implementation Understanding:** Hosted statewide workshops to build district expertise in the CIS Critical Security Controls.
- **Secured Affordable Cybersecurity Services:** Negotiated discounted cybersecurity service offerings from industry leading vendors to reduce local costs.

Next Steps

As SAFE K-12 enters implementation, the following actions outline what districts should do next and how SCDE will support them.

District Responsibilities

1. **Complete Cybersecurity Assessment:** Complete the [CSAT questionnaire](#) to identify local needs. This assessment identifies local gaps and determines the controls your district must prioritize.
2. **Plan Cybersecurity Budgeting for 2026-27:** While there is no program fee for participation under the charter, cybersecurity is now a recurring and essential operational cost for which districts must budget beyond FY26. To help districts plan, SCDE recommends a simple budgeting model:

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

SCDE Next Steps

1. **Publish Service Catalogs:** SCDE will finalize and release statewide K-12 cybersecurity service offerings and vendor catalogs for district planning by
2. **Host Demonstrations and Training:** SCDE will coordinate vendor demonstrations and workshops to support districts in selecting appropriate solutions.

For more information, visit [SAFE K-12: South Carolina's Assurance Framework for Education Cybersecurity](#), or contact the SCDE at safeK12@ed.sc.gov.