Texas Association of School Boards
Legal Services
P.O. Box 400 • Austin, Texas 78767-0400 • 512.467.3610 • 800.580.5345 • legal.tasb.org • legal@tasb.org

Serving Texas Schools Since 1949

School Cybersecurity: Texas Requirements

Published online in TASB School Law eSource

This article focuses on answering questions specific to what Texas law requires school districts to do with respect to cybersecurity.

For basic concepts about cybersecurity, see TASB Legal Services' *School Cybersecurity: Getting Started*. For more information about **required district response to** security breaches, see TASB Legal Services' *School Cybersecurity: Security Breach Notification and Response*.

1. Must Texas school districts adopt a cybersecurity plan?

Yes. TASB Legal Services interprets section 11.175 of the Texas Education Code's requirement for school districts to adopt a cybersecurity "policy" as a requirement to have an administrative plan or procedures to address cybersecurity. TASB Policy Services offers model policy CQB(LOCAL) to direct the district to adopt a cybersecurity plan to secure district cyberinfrastructure against cyberattacks and other cybersecurity incidents, determine cybersecurity risk, and implement mitigation planning. A district cybersecurity plan typically will need to address steps the district may take to prevent, mitigate, resolve, or recover from cybersecurity issues and incidents. A district's cybersecurity plans may not conflict with the Department of Information Resource's (DIR) adopted information security standards for institutions of higher education outlined in Chapter 202 of the Texas Administrative Code. Tex. Educ. Code §§ 11.175(b), (c), 2054.133. See also TASB Model Policy CQB.

2. Must the school board approve the district's cybersecurity plan?

The law does not stipulate that the school board adopt the cybersecurity plan prior to implementation. This makes sense because a district may require flexibility to amend plans in response to unique cybersecurity needs and to make timely adjustments to keep pace with today's cyber threats. However, many districts will have their cybersecurity plans embedded in other districtwide plans, such as their emergency operations plan, that school boards review and approve on a regular basis. Districts should work with their technology directors and school attorneys to identify and organize their cybersecurity protocols into a clear planning document that focuses on increasing cybersecurity and reducing vulnerability to unauthorized access to district data.

3. How might a district go about completing a cybersecurity plan?

In developing or identifying the district's cybersecurity plan, districts may find helpful the Texas Cybersecurity Framework available on the TEA's Texas Gateway Website. This framework contains the security assessment standards created by the DIR that are required for Texas state agencies and institutions of higher education. The framework is not a legal requirement for local governments or school districts. It is, however, a comprehensive checklist that can help districts identify potential sources of vulnerability, determine what additional steps are needed to increase security, discuss how to respond and recover from a breach incident, and organize helpful training for all computer users. A district may choose to mirror the state requirements in its plan but is not required to duplicate it. Districts may also find helpful the DIR's guidance on information security to state agencies on how to create and implement their cybersecurity plans. Some districts may choose to work with private vendors, TASB Risk Management Services, DIR, or other providers who offer cybersecurity assessment services.

4. Will TASB provide a sample or model cybersecurity plan to districts?

No. Cybersecurity plans will look very different for districts around the state. Districts across Texas may face different cybersecurity threats and have varying staff, student enrollment, access points, online content, types of technology support services, network infrastructure, devices and information systems, external agreements, and other technical arrangements. A one-size-fits-all model will not work for every district. Therefore, although TASB Policy Services has created a very basic starting point in its Regulation Resource Manual at CQB(REGULATION), it is not a complete plan. A district will likely find that more district-specific protocols will need to be developed in consultation with its technology director and school attorney.

5. Are cybersecurity coordinators required for each district and what are the duties of a coordinator?

Yes. Every Texas school district superintendent is required to designate a cybersecurity coordinator to serve as a liaison between the district and the Texas Education Agency (TEA) in cybersecurity matters. TEA has asked districts to submit the name and contact information of the designated coordinator to TEA by using the AskTED system. For more information on how to designate the coordinator and how to report cyberattacks to TEA, see TEA's 2019-2020 Cybersecurity Webinars (Sept. 11, 2019).

A school district cybersecurity coordinator must report to TEA any cyberattack or other cybersecurity incident against the district's cyberinfrastructure that constitutes a *breach of system security* and to notify a parent (or person standing in parental relation) whose student's information was involved in the attack or incident for which reporting was required. Tex. Educ. Code § 11.175(d)-(f).

6. Are Texas school districts required to provide cybersecurity training?

Yes. All local governments, including school districts, are required at least once a year to identify employees who have access to district computer systems or databases and require those employees, as well as elected board members, to complete a cybersecurity training program certified by the DIR. Tex. Gov't Code § 2054.5191(a-1); *see also* Tex. Gov't Code § 2054.003(9) (including school district under the definition of *local government*).

If a local government employs a dedicated information resource cybersecurity officer, then the district may offer to its employees and board members a cybersecurity training program that is not DIR-certified so long as the district's program still meets other legal requirements. Tex. Gov't Code § 2054.519(b), (f). The board may select for employees the most appropriate DIR-certified cybersecurity training program or the program offered by a dedicated information resource cybersecurity officer. Tex. Gov't Code § 2054.5191(b). The dedicated information resource cybersecurity officer must complete an online form on the DIR's Website and submit it to the DIR to qualify the district for the exception.

For more information about training deadlines and reporting procedures, see DIR's cybersecurity awareness training and certification requirement Website or email the DIR at TXTrainingCert@dir.texas.gov.

7. What qualifies a person to be a dedicated information cybersecurity officer?

According to the DIR's Website, a dedicated information resources cybersecurity officer must be an employee who has the responsibility for the organization's information security, possesses the training and experience required to administer cybersecurity functions, and has more than 50% of the employee's workload as information security duties.

8. Must school boards report cybersecurity training and require periodic audits?

Yes. A school board must verify and report on the completion of a cybersecurity training program by employees of the school district to the DIR. A board must also require periodic audits of the district to ensure compliance with the law. Tex. Gov't Code § 2054.5191(b).

The DIR will expect all local governments, including school districts, to complete on a web form an acknowledgment that its employees have complied with the security awareness training requirements. The DIR has also made available a Governing Board Acknowledgement Form that boards may complete and retain for their documentation purposes. Please visit the DIR's Website for updates.

9. May the school board choose any cybersecurity training?

No, a school board must approve an appropriate cybersecurity training program that is certified by DIR unless the district employs a dedicated information resources cybersecurity officer and the district offers a cybersecurity training program that complies with the law. Tex. Gov't Code § 2054.5191(b). A district's dedicated information resources cybersecurity officer must file an exception request with the DIR by using its online Local Government Cybersecurity Training & Awareness Program Exception Form and affirm that the district meets the exception requirements.

This document is continually updated, and references to online resources are hyperlinked, at tasb.org/services/legal-services/tasb-school-law-esource/business/documents/school-cybersecurity-texas-requirements.pdf. For more information on this and other school law topics, visit TASB School Law eSource at schoollawesource.tasb.org.