Tex. Educ. Code § 11.175

This document is current through the 2023 Regular Session; the 1st C.S.; the 2nd C.S.; the 3rd C.S. and the 4th C.S. of the 88th Legislature; and the November 7, 2023 general election results.

Sec. 11.175. School Cybersecurity.

(a) In this section:

(1) "Breach of system security" means an incident in which student information that is sensitive, protected, or confidential, as provided by state or federal law, is stolen or copied, transmitted, viewed, or used by a person unauthorized to engage in that action.

(2) "Cyber attack" means an attempt to damage, disrupt, or gain unauthorized access to a computer, computer network, or computer system.

(3) "Cybersecurity" means the measures taken to protect a computer, computer network, or computer system against unauthorized use or access.

(b) Each school district shall adopt a cybersecurity policy to:

(1) secure district cyberinfrastructure against cyber attacks and other cybersecurity incidents; and

(2) determine cybersecurity risk and implement mitigation planning.

(c) A school district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Department of Information Resources under Chapters 2054 and 2059, Government Code.

(d) The superintendent of each school district shall designate a cybersecurity coordinator to serve as a liaison between the district and the agency in cybersecurity matters.

(e) A school district or open-enrollment charter school shall report to the agency or, if applicable, the entity that administers the system established under Subsection (g) any cyber attack or other cybersecurity incident against the school district's or open-enrollment charter school's cyberinfrastructure that constitutes a breach of system security as soon as practicable after the discovery of the attack or incident.

(f) The district's cybersecurity coordinator shall provide notice to a parent of or person standing in parental relation to a student enrolled in the district of an attack or incident for which a report is required under Subsection (e) involving the student's information.

(g) The agency, in coordination with the Department of Information Resources, shall establish and maintain a system to coordinate the anonymous sharing of information concerning cyber attacks or other cybersecurity incidents between participating schools and the state. The system must:

(1) include each report made under Subsection (e);

(2) provide for reports made under Subsection (e) to be shared between participating schools in as close to real time as possible; and

(3) preserve a reporting school's anonymity by preventing the disclosure through the system of the name of the school at which an attack or incident occurred.

(h) In establishing the system under Subsection (g), the agency may contract with a qualified third party to administer the system.

(h–1) Notwithstanding Section 2054.5191, Government Code, only the district's cybersecurity coordinator is required to complete the cybersecurity training under that section on an annual basis. Any other school district employee required to complete the cybersecurity training shall complete the training as determined by the district, in consultation with the district's cybersecurity coordinator.

(i) The commissioner shall adopt rules as necessary to implement this section.

History

Acts 2019, 86th Leg., ch. 605 (S.B. 820), § 1, effective September 1, 2019; Acts 2021, 87th Leg., ch. 1045 (S.B. 1267), § 2, effective June 18, 2021; Acts 2021, 87th Leg., ch. 618 (S.B. 1696), § 1, § 2, effective September 1, 2021; 2023, 88th Leg., H.B. 4595, § 24.001(9), effective September 1, 2023.

End of Document