

4 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

7 CHAPTER 542. CYBERSECURITY PROGRAM

9 (1) "Breach of system security" has the meaning
10 assigned by Section [521.053](#).

13 (3) "Personal identifying information" and "sensitive
14 personal information" have the meanings assigned by Section
15 521.002.

18 (1) has fewer than 250 employees; and

21 Sec. 542.003. CYBERSECURITY PROGRAM SAFE HARBOR: EXEMPLARY
22 DAMAGES PROHIBITED. Notwithstanding any other law, in an action
23 arising from a breach of system security, a person harmed as a
24 result of the breach may not recover exemplary damages from a

business entity to which this chapter applies if the entity demonstrates that at the time of the breach the entity implemented and maintained a cybersecurity program in compliance with Section 542.004.

Sec. 542.004. CYBERSECURITY PROGRAM. (a) For purposes of Section 542.003, a cybersecurity program must:

(1) contain administrative, technical, and physical safeguards for the protection of personal identifying information and sensitive personal information;

(2) conform to an industry-recognized cybersecurity framework as described by Subsection (b);

(3) be designed to:

(A) protect the security of personal identifying information and sensitive personal information;

(B) protect against any threat or hazard to the integrity of personal identifying information and sensitive personal information; and

(C) protect against unauthorized access to or acquisition of personal identifying information and sensitive personal information that would result in a material risk of identity theft or other fraud to the individual to whom the information relates; and

(4) with regard to the scale and scope, meet the following requirements:

(A) for a business entity with fewer than 20 employees, simplified requirements, including password policies and appropriate employee cybersecurity training;

1 (B) for a business entity with at least 20
2 employees but fewer than 100 employees, moderate requirements,
3 including the requirements of the Center for Internet Security
4 Controls Implementation Group 1; and

5 (C) for a business entity with at least 100
6 employees but fewer than 250 employees, compliance with the
7 requirements of Subsection (b).

8 (b) A cybersecurity program under this section conforms to
9 an industry-recognized cybersecurity framework for purposes of
10 this section if the program conforms to:

11 (1) a current version of or any combination of current
12 versions of the following:

13 (A) the Framework for Improving Critical
14 Infrastructure Cybersecurity published by the National Institute
15 of Standards and Technology (NIST);

16 (B) the NIST's special publication 800-171;

17 (C) the NIST's special publications 800-53 and
18 800-53a;

19 (D) the Federal Risk and Authorization
20 Management Program's FedRAMP Security Assessment Framework;

21 (E) the Center for Internet Security Critical
22 Security Controls for Effective Cyber Defense;

23 (F) the ISO/IEC 27000-series information
24 security standards published by the International Organization for
25 Standardization and the International Electrotechnical Commission;

26 (G) the Health Information Trust Alliance's
27 Common Security Framework;

1 (H) the Secure Controls Framework;

2 (I) the Service Organization Control Type 2
3 Framework; or

4 (J) other similar frameworks or standards of the
5 cybersecurity industry;

6 (2) if the business entity is subject to its
7 requirements, the current version of the following:

8 (A) the Health Insurance Portability and
9 Accountability Act of 1996 (42 U.S.C. Section 1320d et seq.);

10 (B) Title V, Gramm-Leach-Bliley Act (15 U.S.C.
11 Section 6801 et seq.);

12 (C) the Federal Information Security
13 Modernization Act of 2014 (Pub. L. No. 113-283); or

14 (D) the Health Information Technology for
15 Economic and Clinical Health Act (Division A, Title XIII, and
16 Division B, Title IV, Pub. L. No. 111-5); and

17 (3) if applicable to the business entity, a current
18 version of the Payment Card Industry Data Security Standard.

19 (c) If any standard described by Subsection (b)(1) is
20 published and updated, a business entity's cybersecurity program
21 continues to meet the requirements of a program under this section
22 if the entity updates the program to meet the updated standard not
23 later than the later of:

24 (1) the implementation date published in the updated
25 standard; or

26 (2) the first anniversary of the date on which the
27 updated standard is published.

1 Sec. 542.005. CONSTRUCTION OF CHAPTER; NO PRIVATE CAUSE OF
2 ACTION. This chapter may not be construed to create a private cause
3 of action or change a common law or statutory duty.

4 SECTION 2. Section 542.003, Business & Commerce Code, as
5 added by this Act, applies only to a cause of action that accrues on
6 or after the effective date of this Act.

7 SECTION 3. This Act takes effect September 1, 2025.

President of the Senate

Speaker of the House

I hereby certify that S.B. No. 2610 passed the Senate on April 30, 2025, by the following vote: Yeas 31, Nays 0.

Secretary of the Senate

I hereby certify that S.B. No. 2610 passed the House on May 28, 2025, by the following vote: Yeas 109, Nays 27, two present not voting.

Chief Clerk of the House

Approved:

Date

Governor