TEXAS BUSINESS & COMMERCE CODE CHAPTER 542

Texas SB 2610 cybersecurity safe harbor: employee tiers and evidence checklist

A plain-English guide for Texas businesses with fewer than 250 employees

Who it covers

Texas Business & Commerce Code Chapter 542 applies to a business entity in Texas that **has fewer than 250 employees** and **owns or licenses computerized data that includes sensitive personal information**. In a lawsuit arising from a breach, a person harmed may not recover exemplary (punitive) damages from that business if it demonstrates that, **at the time of the breach**, it had implemented and maintained a cybersecurity program that complies with §542.004. The safe harbor applies to causes of action that accrue on or after September 1, 2025.

What the program must meet, by headcount

FEWER THAN 20
employees

Simplified requirements, including password policies and appropriate employee cybersecurity training

20 TO 99
employees

Moderate requirements, including CIS Controls Implementation Group 1

100 TO 249
employees

An industry-recognized cybersecurity framework, as listed in §542.004(b)

ALL TIERS Administrative, technical and physical safeguards for personal and sensitive personal information (§542.004)

Requirements are summarized. See §542.004 for the full text, including the frameworks listed in subsection (b) and how to keep pace when a framework is updated.

What it does not do

It removes exemplary (punitive) damages only.	Actual damages remain.
It does not replace other duties.	Breach notification under Texas law, and HIPAA, GLBA, PCI DSS or the Texas Data Privacy and Security Act where they apply, are unchanged.
It does not affect class actions.	Chapter 542 does not change whether a case can be certified as a class action.
It is not automatic.	The business must demonstrate the program existed and was maintained at the time of the breach.

Evidence checklist

Use this as a worksheet. If a breach happens, the question is not whether you had a policy, but whether you can show the program was in place and maintained at the time.

Evidence	Reference	Owner	Date verified
Written cybersecurity program, naming your framework and tier	§542.004 · your tier		
Administrative, technical and physical safeguards, documented	§542.004		
Password policy	All tiers		
Employee cybersecurity training records	All tiers		
Inventory of where sensitive data is stored A DATA SCAN HELPS	CIS 3.2 · NIST CSF ID.AM-07		
Review of broad access to sensitive data, and the changes made A DATA SCAN HELPS	CIS 3.3		
Approved disposal of aged data, checked against legal holds A DATA SCAN HELPS	CIS 3.4 and 3.5		
Review dates set under your framework, and after material changes	Your framework		

A data scan helps produce three items: a dated inventory, a list of broad access to sensitive files, and a list of aged files. The changes you make, the approvals and the follow-up checks each need their own record. CIS Control 3.2 asks for the data inventory to be reviewed at least annually.

Start with the inventory, free

USC Data will scan up to 20,000 files across SharePoint, email or a file server, inside your own environment, and give you a dated report you can file as evidence.

Get the free 20,000-file scan

Sources: Texas Business & Commerce Code, Chapter 542; S.B. 2610, enrolled version; CIS Critical Security Controls v8.1; NIST Cybersecurity Framework 2.0. **General information, not legal advice.** Updated November 2026. Have your attorney confirm how Chapter 542 applies to your business. A data scan supports a cybersecurity program; it does not by itself qualify a business for the safe harbor.