# Texas SB 2610 Cybersecurity Safe Harbor

*A Comprehensive Guide for Law Firms & Small Businesses*

*Effective September 1, 2025 | Prepared by EmailMeNow IT Consulting | April 2026*

## Executive Summary

Senate Bill 2610 (SB 2610), signed into law by Governor Greg Abbott on June 20, 2025 and effective September 1, 2025, establishes a powerful legal safe harbor for Texas businesses with fewer than 250 employees. The law shields qualifying organizations from **exemplary (punitive) damages** in civil lawsuits arising from data breaches, provided they maintain a documented cybersecurity program aligned with recognized industry frameworks such as NIST CSF, ISO 27001, or CIS Controls.

**Key Benefit:** By demonstrating reasonable cybersecurity practices at the time of a breach, businesses can significantly reduce their financial exposure in litigation while fulfilling ethical and regulatory obligations under TDRPC Rule 1.05 and Texas data breach notification laws.

## Legislative Background & Purpose

Texas joins a growing number of states (including Ohio, Utah, and others) that have enacted cybersecurity safe harbor legislation. The bill adds **Chapter 542** to the Texas Business & Commerce Code and was designed to address the unique challenges faced by small and mid-sized businesses (SMBs), which often lack the resources of large enterprises yet face the same sophisticated cyber threats.

Lawmakers recognized that punitive damages can be disproportionate for smaller organizations that have made good-faith efforts to secure client and customer data. SB 2610 incentivizes proactive investment in cybersecurity by offering predictable liability protection in exchange for documented, framework-aligned security programs.

## Who Qualifies for Safe Harbor Protection?

To be eligible, a business must meet **all** of the following criteria at the time of the breach:

- Be a **Texas business entity** (headquartered or operating in Texas).

- Have **fewer than 250 employees** (full-time equivalents).
- Own or license **computerized data** that includes **sensitive personal information** (as defined in Tex. Bus. & Com. Code §521.002).
- Maintain a qualifying **cybersecurity program** (detailed below) that was in place and operational when the breach occurred.

*Note: Businesses with 250 or more employees are not covered by this safe harbor and must rely on other defenses.*

## What Protection Does SB 2610 Provide?

If a qualifying business demonstrates that it maintained a compliant cybersecurity program at the time of a breach of system security, a plaintiff **may not recover exemplary damages** (punitive damages) in a civil action arising from that breach.

**Important Limitations:**

- Does **not** eliminate liability for actual/compensatory damages, medical monitoring, or other economic losses.
- Does **not** prevent regulatory enforcement actions by the Texas Attorney General (e.g., under breach notification rules).
- Does **not** create a private right of action or alter existing common-law duties.
- Protection is lost if the business cannot **prove** the program existed and was maintained (documentation is critical).

## Core Requirements of a Qualifying Cybersecurity Program

Per Texas Business & Commerce Code §542.224, a cybersecurity program must satisfy four pillars:

### 1. Administrative, Technical, and Physical Safeguards

The program must include layered controls covering policies/procedures (administrative), technology solutions such as encryption, access controls, and monitoring (technical), and physical security measures (facility access, device security).

### 2. Conformance to a Recognized Industry Framework

The program must align with at least one of the following (current versions or combinations permitted):

- NIST Cybersecurity Framework (CSF) or SP 800-53 / 800-171 / 800-172
- ISO/IEC 27001 series
- CIS Critical Security Controls (especially IG1 for smaller firms)
- SOC 2 Trust Services Criteria
- Secure Controls Framework (SCF)
- Industry-specific: HIPAA/HITECH, GLBA, PCI DSS, FISMA, FedRAMP, HITRUST CSF (if applicable to the entity)

### 3. Specific Protective Purposes

The program must be *designed to*: (A) protect the security of personal identifying information and sensitive personal information; (B) protect against threats or hazards to its integrity; and (C) protect against unauthorized access or acquisition that would result in a material risk of identity theft or other fraud.

### 4. Scaled to Business Size (Tiered Requirements)

Requirements are proportionate to organizational size and resources:

| Employee Count | Required Cybersecurity Measures | Example Framework |
|---|---|---|
| Fewer than 20 | Simplified / Basic<br>• Password policies<br>• Employee cybersecurity training<br>• Basic administrative, technical & physical safeguards | NIST CSF (basic profile)<br>or CIS Controls IG1 essentials |
| 20 – 99 | Moderate (CIS Controls IG1)<br>• Essential cyber hygiene controls<br>• Documented policies & procedures<br>• Regular employee training & awareness | CIS Controls Implementation Group 1 (IG1) – "Essential Cyber Hygiene" |
| 100 – 249 | Full Framework Compliance<br>• Comprehensive controls across all domains<br>• Risk assessments, incident response, continuous monitoring | NIST CSF, ISO 27001, SOC 2,<br>or full CIS Controls IG1+IG2 |

*Note: Businesses already subject to HIPAA, GLBA, PCI DSS, or similar regulatory frameworks may leverage their existing compliance programs to satisfy SB 2610 requirements.*

## Documentation & Maintenance Requirements

The safe harbor is only as strong as your ability to **prove** compliance. Recommended documentation includes:

- Written cybersecurity policies and procedures (acceptable use, incident response, data classification, vendor management).
- Employee training records and acknowledgment forms (annual minimum).
- Risk assessments, vulnerability scans, and penetration test reports (as applicable by tier).
- Network diagrams, asset inventories, and data flow maps.
- Incident response plans and post-incident review logs.
- Annual program reviews and updates (recommended even if not strictly required).
- Evidence of framework mapping (e.g., NIST CSF or CIS Controls spreadsheet showing control implementation status).

**Best Practice:** Conduct and document an annual cybersecurity program review. Update controls promptly when frameworks are revised (you generally have up to one year after publication of an updated standard).

## Special Relevance for Texas Law Firms

Texas law firms handle highly sensitive client information (privileged communications, financial data, PII) and are explicitly subject to **TDRPC Rule 1.05** (Confidentiality of Information), which requires "reasonable efforts" to prevent unauthorized disclosure. SB 2610 provides a concrete, objective standard for what "reasonable" means in the cybersecurity context.

Additionally, **ABA Model Rule 1.1 Comment 8** (adopted in Texas) requires lawyers to understand the benefits and risks of technology, including cybersecurity. Implementing an SB 2610-compliant program simultaneously satisfies ethical obligations, reduces malpractice exposure, protects client trust, and limits punitive damages in the event of a breach.

Law firms with 20–99 employees (common size) should prioritize **CIS Controls IG1** implementation as the most straightforward path to safe harbor while meeting TDRPC expectations.

## Recommended Steps to Achieve Safe Harbor

**Step 1:** Determine your employee tier and applicable regulatory overlays (HIPAA, PCI, etc.).

**Step 2:** Conduct a gap assessment against your chosen framework (NIST CSF or CIS Controls recommended for most firms).

**Step 3:** Develop or update policies, procedures, and technical controls; document everything.

**Step 4:** Implement required training and awareness programs; maintain records.

**Step 5:** Establish ongoing monitoring, vulnerability management, and incident response capabilities.

**Step 6:** Perform an annual program review and update the program to reflect changes in business operations or framework updates.

**Step 7:** Engage a qualified third party (such as EmailMeNow IT) for independent validation or remediation support if needed.

**Ready to protect your firm and qualify for SB 2610 safe harbor? EmailMeNow IT Consulting provides zero-knowledge cybersecurity audits, CIS Controls / NIST implementation roadmaps, policy templates, and ongoing compliance support specifically tailored for Texas law firms. Contact us at +1 (979) 472-3693 or visit emailmenow.com to schedule your free audit today.**

### Disclaimer

*This guide is for informational purposes only and does not constitute legal advice. Consult qualified Texas counsel for advice specific to your situation. SB 2610 safe harbor protection depends on the specific facts of each case and the quality of documentation maintained by the business entity.*

### Primary Sources

- *Texas Senate Bill 2610 (89th Legislature) – Enrolled version, effective Sept. 1, 2025*
- *Texas Business & Commerce Code Chapter 542 (as added by SB 2610)*
- *Analyses: Spencer Fane LLP, Center for Internet Security (CIS), HIPAA Journal, Texas Policy Research*