Texas Safe Harbor Compliance Guide for Small Businesses

Rashmi Sheel

Texas Safe Harbor Compliance Guide for Small Businesses

Protect Your Business. Protect Your Reputation.

(Law effective September 1, 2025)

1. Why Small Businesses Are Prime Targets of Cybercrime

Small businesses are often seen as “low-hanging fruit” because they underestimate their risk, have limited budgets, and lack written policies, backups, or staff training.

Recent studies highlight the risks:

- 68% of all breaches in 2024 involved human error or social engineering. (Verizon DBIR 2024)
- 44% of breaches in 2025 involved ransomware. (Verizon DBIR 2025)
- ~30% of incidents involved third-party or vendor compromise. (Verizon DBIR 2025)
- The average breach cost for small and mid-sized businesses ranged from $120,000 to $1.24 million. (BigID 2024)
- 60% of small firms closed within six months of a serious cyber incident. (National Cybersecurity Alliance)

2. What Is the Texas Safe Harbor Law

The Texas Safe Harbor Law (Senate Bill 2610) rewards small businesses that make a good-faith effort to secure and document their data.
If you experience a cyberattack but can show that you had a reasonable cybersecurity program in place, the law can limit punitive damages in a lawsuit.
The law encourages adoption of written cybersecurity programs scaled to your business size and risk. It's modeled after similar successful laws in Ohio and Utah.

3. Why This Matters to Small Businesses

Cyberattacks on small businesses are rising every year. Most rely on cloud storage, email, and online payments but lack written policies or documented controls. When a breach occurs:
• Costs can reach hundreds of thousands of dollars.
• Insurance claims may be denied if you cannot prove the security controls listed in your policy—such as MFA, backups, monitoring, and firewalls—were implemented and documented.
• Rebuilding customer trust takes time and resources.
Safe Harbor gives business owners legal and insurance protection when they can show written policies, training logs, and backup documentation.
(Sources: National Cybersecurity Alliance; Verizon 2024 DBIR; Coalition Cyber Insurance Claims Report 2024)

4. Who This Law Applies To

Safe Harbor applies to any business that collects or stores personal information about customers, employees, or vendors, including:
• Restaurants and retailers accepting credit cards
• Real estate offices and mortgage brokers
• Healthcare and dental clinics
• Nonprofit organizations
• Accounting and law firms
If you store or process customer or employee data, this law applies to you.

5. The Three Tiers of Compliance

The Three Tiers of Compliance – Texas Safe Harbor Law

Tier & Business Size	Goal & Framework	What to Do	What to Document
Tier 1 – Small Businesses (1–19 employees)	**Goal:** Basic cyber hygiene **Framework:** Reasonable Cybersecurity Program	• Enable MFA and use strong passwords. • Keep antivirus on all devices and apply monthly updates. • Back up data daily or weekly; test restores monthly. • Secure Wi-Fi and routers with strong passwords. • Provide annual employee cybersecurity training.	• Password Policy • Acceptable Use Policy • Backup Checklist • Training Log
Tier 2 – Medium Businesses (20–99 employees)	**Goal:** Structured security program **Framework:** CIS Controls or NIST CSF	**Includes all Tier 1 controls, plus:** • Managed endpoint protection and automated patching. • Business-class firewall and VPN for remote work. • 24/7 monitoring and alert response. • Quarterly backup tests and vendor reviews.	**Includes all Tier 1 documentation, plus:** • Written Information Security Plan (WISP) • Password & Access Policy • Vendor Risk Policy • Incident Response Plan
Tier 3 – Large Small Businesses (100–249 employees)	**Goal:** Comprehensive alignment **Framework:** NIST SP 800-171 or ISO 27001	**Includes all Tier 1 & Tier 2 controls, plus:** • Enterprise Endpoint Protection with threat monitoring. • Next-generation firewall and network segmentation. • Continuous logging and SIEM analysis. • Monthly vulnerability scans and patch tracking. • Annual disaster recovery testing.	**Includes all Tier 1 & Tier 2 documentation, plus:** • Governance & Risk Policy • Password & MFA Policy • Encryption Policy • Backup and Disaster Recovery Plan • Annual Audit Review

6. Cloud and Vendor Responsibilities

Even if you use third-party applications like Microsoft or Google, you remain responsible for your data under the shared responsibility model.

- Ask Vendors:
- What is backed up and how often (RPO/RTO)?
- Do you test restores and provide reports?
- Is data encrypted? Is MFA required for administrators?
- Where is data stored, and is it geo-redundant?
- What is your incident notification timeframe (SLA)?
- Do you hold SOC 2 or ISO 27001 certification?
- How will I retrieve my data if we terminate the service?

Microsoft Backup: Microsoft Backup is a paid service. You must enable it yourself and ensure backups and restores are tested—or use a third-party backup provider that performs and documents restore tests. Without written proof of retention and restore testing, your Safe Harbor or insurance protection may weaken.

7. Credit Cards, Insurance, and the Law

If you accept credit cards, you handle sensitive information. PCI DSS v4.0 requires firewalls, MFA, and network separation for payment systems (PCI Security Standards Council).

Cyber-insurance carriers may deny or reduce coverage if you cannot prove that the controls listed in your policy—such as MFA, backups, monitoring, or firewalls—were deployed and documented.

Safe Harbor strengthens your defense by proving reasonable cybersecurity practices with written evidence.

8. Building a Cybersecurity Program in 7 Steps

1. List all systems, vendors, data, and users.
2. Write brief policies (password/MFA, backup, acceptable use, incident plan).
3. Train employees annually.
4. Enable MFA, backups, and updates; assign responsibility.
5. Test restores and save proof (screenshots, reports).
6. Store everything in a “Cybersecurity Records” folder or binder.
7. Review annually and update after major changes or incidents.

9. Frequently Asked Questions

- **Q:** If I just take credit cards, does this apply?
- **A:** Yes. Credit card data is sensitive information. PCI compliance and Safe Harbor overlap. With PCI your network security matters.
- **Q:** My data is in the cloud. Am I safe?
- **A:** Not automatically. Enable backups, verify restores, and use MFA. Get with vendor and discuss data security as in section 6.
- **Q:** Does Microsoft automatically back up my data?
- **A:** No. Microsoft offers a paid backup service, but you must activate and test it regularly.
- **Q:** Will Safe Harbor stop all lawsuits?
- **A:** No. It limits punitive damages but not compensatory or regulatory penalties.
- **Q:** What if I have an IT provider?
- **A:** You still need proof—contracts, documented policies, procedures and training records.
- **Q:** How often should I review my program?
- **A:** Once per year or after major changes in staff, systems, or vendors.

10. What Records to Keep

- Cybersecurity Policies (WISP, Password, MFA, Backup, Acceptable Use)
- Employee Training Logs
- Backup and Restore Reports
- Vendor Contracts and Security Reviews
- Insurance Attestations and Renewals
- Patch and Vulnerability Scan Reports
- Annual Review Sign-off

11. Real-World Case Studies

CDK Global Ransomware Attack (2024)

A cloud software provider for car dealerships was hit by ransomware, disrupting about 15,000 dealerships. Dealers went offline for days; industry losses exceeded $1 billion.

Sources: TechTarget | CBS News | Detroit Free Press

Microsoft 365 License Lapse (2023)

A nonprofit lost access to SharePoint and OneDrive when its Microsoft 365 grant license expired, and it had no backup.

Sources: Microsoft Q&A | Microsoft Tech Community

12. Benefits of Safe Harbor Compliance

- Legal protection from punitive damages after a breach
- Fewer insurance claim disputes
- Builds customer and partner trust
- Easier contract and audit approvals
- Demonstrates good faith and accountability

13. Source References

- Texas Senate Bill 2610 (Safe Harbor Law)
- Verizon Data Breach Investigations Reports 2024 & 2025
- PCI DSS v4.0 (Payment Card Industry Standards)
- Microsoft Shared Responsibility Model & Backup Overview
- Coalition Cyber Insurance Claims Report 2024
- TechTarget, CBS News, Detroit Free Press (CDK Global case)
- Microsoft Q&A and Tech Community (M365 case)
- BigID 2024 SMB Breach Cost Analysis
- National Cybersecurity Alliance (StaySafeOnline.org)

Texas Safe Harbor Compliance Guide for Small Businesses

About Rashmi Sheel

Rashmi Sheel is a dedicated advocate for small business cybersecurity and the owner of CMIT Solutions of Sugar Land. With a strong background in IT leadership and compliance advisory, Rashmi helps local organizations develop practical, cost-effective cybersecurity programs that align with both legal standards and business operations. Her mission is to make cybersecurity accessible and manageable for growing businesses.

Texas Safe Harbor Compliance Guide for Small Businesses

About CMIT Solutions

CMIT Solutions is a nationally recognized IT services provider with over 25 years of experience delivering IT solutions to small and mid-sized businesses. With more than 250 locations across North America, CMIT combines the personal service of a local provider with the resources of a national firm.

Our offerings include proactive IT management, cybersecurity protection, cloud solutions, and compliance support tailored to industry-specific needs. CMIT is known for its reliability, responsiveness, and commitment to helping businesses stay secure, productive, and resilient in a rapidly evolving digital landscape.

CMIT Solutions of Sugar Land

rsheel@cmitsolutions.com | (281) 656-1099

https://cmitsolutions.com/sugarland

Compliance is more than paperwork—it's peace of mind.