Texas SB 2610 Cybersecurity Readiness Checklist

This checklist helps Texas organizations under 250 employees document technical controls that may support an SB 2610 program file. It is educational material only.

Program basics to document

- Named owner for cybersecurity decisions and annual review dates
- Inventory of systems and vendors that store personal or client data
- Access control policy (provisioning, review, removal) and MFA requirements
- Backup, restore, and incident reporting procedures
- Security awareness training schedule and completion records

Email and domain evidence (automated scan)

- SPF, DKIM, and DMARC posture for your primary sending domain
- TLS and transport settings for inbound and outbound mail
- Certificate expiry monitoring for public web and mail hosts
- Documented change log when DNS or mail records are updated

Annual readiness review

Re-run your scan, attach results to your program binder, and note remediation items. Compare automated reports over time using Watch plans when you need ongoing monitoring.

Free scan: audit.emailmenow.com · Automated products: emailmenow.com/services

---

SB 2610 may help limit exemplary damages for eligible businesses that maintain a documented cybersecurity program; not legal advice or a guarantee.