2026 Texas SMB Cybersecurity Checklist

30-Item Security Checklist for Central Texas Small Businesses · Free Resource from Computek · computekonline.com

How to use this checklist: Work through each category and check off items your business has implemented. Any unchecked item is a potential vulnerability. Prioritize gaps by risk level. **Recommended review frequency: quarterly.** Texas regulations and the threat landscape change rapidly — stay current.

☐ 1. Access Control & Authentication

- ☐ **Multi-factor authentication (MFA) on ALL accounts**
  Email, M365, banking, VPN, cloud services — no exceptions
- ☐ **Strong password policy: 12+ characters, complexity required**
  Use a business password manager: LastPass, 1Password, Bitwarden
- ☐ **Admin privileges limited to necessary personnel only**
  Least privilege: each user gets only the access they need
- ☐ **Employee offboarding: all accounts disabled within 24 hours**
  Email, cloud apps, door codes, remote access — all of them
- ☐ **Guest Wi-Fi separated from business network**
  Visitors/personal devices must never share your business LAN
- ☐ **Single sign-on (SSO) or identity provider deployed for SaaS apps**
  Reduces credential sprawl; simplifies offboarding

☐ 2. Network & Endpoint Security

- ☐ **Business-grade firewall installed & actively monitored**
  Consumer routers are NOT sufficient — Fortinet, SonicWall, etc.
- ☐ **All endpoints protected by EDR/antivirus (not just Windows Defender)**
  Laptops, desktops, phones, tablets — every device on the network
- ☐ **Automatic OS & software updates enabled across all devices**
  Unpatched systems are the #1 ransomware entry point
- ☐ **RDP disabled or protected behind VPN + MFA**
  Exposed RDP is attacked within minutes of being discovered online
- ☐ **Dark web monitoring active for company email domains**
  Get alerted when employee credentials appear in breach databases
- ☐ **Wireless networks secured with WPA3 or WPA2-Enterprise**
  Change default router passwords; don't broadcast your business name in SSID
- ☐ **Network segmentation: servers isolated from workstations**
  Limits lateral movement if one machine is compromised

☐ 3. Data Protection & Backup

- ☐ **Backups follow the 3-2-1 rule**
  3 copies · 2 different media types · 1 stored offsite or cloud
- ☐ **Backups tested & restored quarterly — not just stored**
  An untested backup is not a backup. Run restore drills every 90 days.
- ☐ **Sensitive data encrypted at rest and in transit**
  Full-disk encryption (BitLocker/FileVault) + TLS on all data transfers
- ☐ **Data classification policy in place**
  Public / Internal / Confidential / Restricted — label your data
- ☐ **Disaster recovery plan documented & reviewed annually**
  Who does what, in what order, to restore operations after an incident
- ☐ **Cloud storage permissions audited — no over-sharing**
  Audit Google Drive/SharePoint/OneDrive sharing settings quarterly

☐ 4. Employee Training & Awareness

- ☐ **Annual cybersecurity awareness training for all staff**
  Phishing, password hygiene, physical security, social engineering
- ☐ **Phishing simulations conducted at least quarterly**
  Simulated phishing finds at-risk employees before real attackers do
- ☐ **Clear policy for reporting suspicious emails/calls/activity**
  A no-blame culture: fear of punishment delays critical reporting
- ☐ **Social engineering training: vishing, pretexting, CEO fraud**
  Train staff to verify wire transfers & data requests via a second channel
- ☐ **Acceptable Use Policy (AUP) signed by all employees & contractors**
  Covers personal device use, remote work, cloud app restrictions

☐ 5. Texas-Specific Compliance

- ☐ **Texas Identity Theft Enforcement & Protection Act (TIPEA) reviewed**
  Requires reasonable security measures protecting sensitive personal info
- ☐ **Texas Privacy Protection Act (TXPPA) requirements assessed**
  Know what personal data you collect, how it's used, how to respond to requests
- ☐ **HIPAA security measures in place (if handling PHI / healthcare clients)**
  Risk analysis, access controls, audit logs, breach response plan required
- ☐ **Incident response plan includes TX 60-day breach notification requirement**
  TX law: notify affected individuals within 60 days of discovering a breach
- ☐ **Cyber liability insurance coverage reviewed & confirmed adequate**
  Standard BOP policies usually do NOT cover ransomware or data breach costs
- ☐ **Third-party vendor security assessed (supply chain risk)**
  Texas law may hold you liable for breaches caused by your vendors

☐ 512-869-1155 · computekonline.com
1614 Williams Dr, Suite 105 · Georgetown, TX 78628
Serving Central Texas since 2001 · Woman-owned business