ITBIZTEK

itbiztek.com

IT Compliance Checklist for Toronto Businesses

An eight-item baseline for 2026 SMB programs

The eight controls that matter

1 Document your data inventory

List every system holding personal information. Where it lives, who can access it, retention rules. Foundation of every other control.

2 Enforce multi-factor authentication

MFA on email, VPN, admin accounts. App or hardware-based preferred. SMS is the weakest method due to SIM-swap risk.

3 Run modern endpoint protection

Endpoint Detection and Response (EDR) on every device. Microsoft Defender for Business, CrowdStrike Go, or SentinelOne. 4 to 15 dollars per device per month.

4 Back up everything, test the restores

3-2-1 rule: three copies, two media types, one off-site and immutable. Quarterly restore drill or your backup is theoretical.

5 Patch operating systems and apps

Automated patch management closes the gap. Adobe Reader, browsers, Java, remote access tools are the usual exploit targets.

6 Quarterly access review

Each manager confirms who on their team should have what. Stale accounts and excessive permissions surface in 30 minutes per quarter.

7 Written, rehearsed incident response plan

Two pages, fits on a clipboard. Who decides, who calls the lawyer, who calls the Privacy Commissioner. Tabletop twice per year.

8 Train your people, monthly

Annual training is the floor. Monthly micro-training plus simulated phishing is what works. Track click rate over time.

Quarterly review cadence

Q1: Test backup restores. Run access review. Update incident response plan with any organizational changes.
Q2: Run a phishing simulation. Review patching gaps. Refresh staff training.
Q3: External cybersecurity assessment. Update data inventory. Test incident response with a tabletop exercise.
Q4: Annual policy review. Renew cyber insurance with documented controls. Plan investments for the year ahead.

Need help working through this checklist? ITBizTek serves Toronto and the GTA.