IT Security Checklist

For Calgary & Airdrie Businesses

Protect your business in 30 minutes | 7 categories | 42 checkpoints

This checklist covers the security fundamentals every Calgary and Airdrie business should have in place. Use it as a self-audit or bring it to your next IT review. If you find gaps, we can help.

1. Identity & Access Management

[ ] Multi-factor authentication (MFA) enforced on all user accounts
Microsoft now requires MFA for all M365 tenants. If yours isn't enforced, you're exposed.

[ ] Conditional access policies configured for location and device compliance
Block sign-ins from unexpected countries and unmanaged devices.

[ ] Admin accounts are separate from daily-use accounts

[ ] Former employee accounts disabled within 24 hours of departure

[ ] Password policy enforces 14+ character minimum or passphrase

[ ] Privileged access reviewed quarterly
Who has Global Admin? Who can access financials? Audit it.

2. Email & Phishing Defence

[ ] SPF, DKIM, and DMARC records configured and enforced

[ ] Anti-phishing policies active in Microsoft Defender or equivalent
Impersonation protection for executives and finance staff.

[ ] External email tagging enabled (banner on external messages)

[ ] Attachment sandboxing / Safe Attachments enabled

[ ] Forwarding rules audited monthly (no silent auto-forwards to external)

[ ] Phishing simulation training run at least quarterly

3. Endpoint Protection & Device Management

[ ] EDR (Endpoint Detection & Response) deployed on all endpoints

[ ] Devices enrolled in management platform (Intune, etc.)

[ ] OS and application patching automated with 14-day compliance window

[ ] Local admin rights removed from standard user accounts

[ ] Full-disk encryption enabled (BitLocker / FileVault)

[ ] USB and removable media policies enforced
Block or audit USB storage to prevent data exfiltration.

4. Data Protection & Backup

[ ] Cloud backup configured for M365 mailboxes, SharePoint, and OneDrive

[ ] On-premises backup with offsite or cloud copy (3-2-1 rule)

[ ] Backup recovery tested at least quarterly

[ ] Sensitivity labels applied to confidential documents

[ ] Data Loss Prevention (DLP) policies active for email and file sharing
Prevent accidental sharing of SINs, credit card numbers, or client data.

[ ] Retention policies configured to meet regulatory requirements

5. Network & Infrastructure Security

[ ] Firewall firmware current and rules reviewed annually

[ ] Wi-Fi uses WPA3 or WPA2-Enterprise with segmented guest network

[ ] VPN or ZTNA (Zero Trust Network Access) for remote workers

[ ] Network segmentation between staff, IoT, and guest devices

[ ] DNS filtering active to block known malicious domains

[ ] Remote desktop (RDP) disabled or restricted to VPN-only access

6. Incident Response & Business Continuity

[ ] Incident response plan documented and accessible offline

[ ] Key contacts list (IT provider, insurance, legal) current and printed

[ ] Cyber insurance policy in place and reviewed annually

[ ] Ransomware playbook tested with tabletop exercise
When did you last simulate a ransomware scenario with your team?

[ ] Recovery Time Objective (RTO) and Recovery Point Objective (RPO) defined

[ ] Business continuity plan tested for office-down and cloud-down scenarios

7. Compliance & Governance

[ ] Acceptable Use Policy signed by all employees annually

[ ] Industry compliance requirements documented (PIPEDA, PCI-DSS, etc.)
Alberta businesses handling personal data must comply with PIPEDA at minimum.

[ ] Security awareness training completed by all staff annually

[ ] Vendor and third-party access reviewed quarterly

[ ] IT asset inventory current (hardware, software, licences)

[ ] Annual IT security assessment with external review

How Did You Score?

Score	Rating	What It Means
36 - 42	**Strong**	Your security posture is solid. Focus on maintaining and testing.
25 - 35	**Moderate**	Key protections in place but gaps exist. Prioritize the unchecked items.
15 - 24	**At Risk**	Significant exposure. An IT assessment would help prioritize fixes.
0 - 14	**Critical**	Immediate action needed. Your business is highly exposed to common threats.

Need Help Closing the Gaps?

IT Works MSP offers a **free IT assessment** for Calgary and Airdrie businesses. We review your environment against this checklist and more, then give you an honest recommendation with no obligation to proceed.

Book your assessment: itworksmsp.ca/contact | 1 (800) 566-4188 | info@itworksmsp.ca

Based in Airdrie, Alberta. Serving Calgary, Edmonton, and beyond.