VisioClara

MICROSOFT CLOUD & AI PARTNER

SECURITY CHECKLIST

The Canadian SMB & Startup Microsoft Security Checklist

A practical Microsoft 365 + Azure security checklist for Canadian teams

Vision-led. Trust-built. Clarity-driven.

BUILT FOR CANADIAN TEAMS

PIPEDA · Quebec Law 25 · Azure Canada Central / Canada East

Microsoft, made simple.

visioclara.com · info@visioclara.com · Toronto, Canada

Security is a growth enabler

HOW TO USE THIS CHECKLIST

Strong security is not a tax on growth — it is what unlocks it.

For Canadian startups and SMBs, good security wins customer trust, clears vendor and enterprise procurement reviews faster, protects the data your business runs on, and keeps you resilient when something goes wrong. The good news: if you are already on Microsoft 365 or Azure, most of the controls you need are built in and waiting to be switched on — no new platform required.

This checklist turns Microsoft's security surface into plain, do-able steps. Work through each domain and tick the boxes. Use the tiers to pace yourself — you do not need to do everything at once.

Crawl → Walk → Run: pace your rollout

Crawl — essential controls every team should have on day one.

Walk — strengthen and automate as your team and data grow.

Run — mature, monitored, and audit-ready for enterprise deals.

The Canadian angle

Throughout, we flag where controls support **PIPEDA** and **Quebec Law 25** obligations and where to keep data in **Azure Canada Central / Canada East** for data residency. Figures shown as [add stat] are placeholders for your own verified numbers.

01 Identity & access

MICROSOFT ENTRA ID

Identity is the new perimeter. Lock down who can sign in, from where, and with what.

- [ ] **Enforce multi-factor authentication (MFA)** for every user — no exceptions. — CRAWL
- [ ] **Require phishing-resistant MFA** (authenticator app or FIDO2 keys) for all administrators. — CRAWL
- [ ] **Block legacy authentication** protocols (POP, IMAP, SMTP basic auth) that bypass MFA. — CRAWL
- [ ] **Secure and separate admin accounts** — use dedicated, cloud-only admin identities. — CRAWL
- [ ] **Turn on Conditional Access** policies for device, location, and sign-in risk. — WALK
- [ ] **Apply least privilege** — grant each role only the access it genuinely needs. — WALK
- [ ] **Enable self-service password reset** with strong verification to cut helpdesk risk. — WALK
- [ ] **Use Privileged Identity Management (PIM)** for just-in-time, time-boxed admin access. — RUN
- [ ] **Review guest and external identities** regularly and remove stale access. — RUN

Why it matters: the majority of breaches start with a compromised identity. MFA and blocking legacy auth are the single highest-return controls you can enable today.

02 Devices & apps

MICROSOFT INTUNE + DEFENDER FOR ENDPOINT

Only healthy, managed devices should reach company data — laptops and phones alike.

- [ ] **Require disk encryption** (BitLocker / FileVault) on every device. — CRAWL
- [ ] **Deploy Microsoft Defender for Endpoint** to all workstations for next-gen antivirus & EDR. — CRAWL
- [ ] **Enrol company and BYOD devices** in Microsoft Intune for central management. — WALK
- [ ] **Enforce device compliance policies** (encryption, PIN, minimum OS, jailbreak checks). — WALK
- [ ] **Apply app protection policies (MAM)** to contain company data on personal phones. — WALK
- [ ] **Automate OS and app patching** with Intune update rings. — WALK
- [ ] **Restrict app installs** to approved, trusted sources. — RUN
- [ ] **Remotely lock or wipe** lost and stolen devices, and off-board leavers cleanly. — RUN

03 Email & collaboration

MICROSOFT DEFENDER FOR OFFICE 365

Email and sharing are the top attack paths. Filter threats and set clear sharing guardrails.

- [ ] **Configure anti-spam and anti-malware** policies at recommended (or stricter) levels. — CRAWL
- [ ] **Turn on anti-phishing** policies with impersonation and spoof protection. — CRAWL
- [ ] **Enable Safe Links** to scan and rewrite URLs at click time. — CRAWL
- [ ] **Enable Safe Attachments** to detonate unknown files in a sandbox before delivery. — WALK
- [ ] **Authenticate your domains** with SPF, DKIM, and DMARC to stop spoofing. — WALK
- [ ] **Set external-sharing guardrails** in SharePoint, OneDrive, and Teams. — WALK
- [ ] **Add external-sender warning banners** to inbound mail. — WALK
- [ ] **Run phishing simulations** and short training to build a human firewall. — RUN

Guardrail, don't block: tune external sharing so collaboration still flows — expiring links, allow-listed domains, and view-only defaults beat a hard 'no'.

04 Data protection & compliance

MICROSOFT PURVIEW

Know your data, label it, and stop it leaving — the backbone of PIPEDA & Law 25 readiness.

- [ ] **Create sensitivity labels** (Public, Internal, Confidential) and publish them to users. — CRAWL
- [ ] **Keep Canadian data in-region** — Azure Canada Central / Canada East for data residency. — CRAWL
- [ ] **Turn on Data Loss Prevention (DLP)** for email, Teams, and endpoints. — WALK
- [ ] **Map where personal & regulated data lives** with a simple data inventory. — WALK
- [ ] **Protect personal information** to align with PIPEDA and Quebec Law 25 obligations. — WALK
- [ ] **Configure retention and records** policies so data is kept — and deleted — on schedule. — WALK
- [ ] **Auto-apply labels & encryption** to sensitive content and enable audit logging. — RUN
- [ ] **Document a privacy-breach response** process — Law 25 requires notification. — RUN

PIPEDA & Law 25: both expect you to know what personal data you hold, protect it, and be ready to report a breach. Labels, DLP, and Canadian data residency cover the essentials.

05 Azure security

IF YOU BUILD ON AZURE

Extend Zero Trust to your cloud workloads: protect identities, networks, secrets, and posture.

- [ ] **Turn on Microsoft Defender for Cloud** across all subscriptions for posture & workload protection. — CRAWL
- [ ] **Store secrets, keys, and certificates** in Azure Key Vault — never in code or config. — CRAWL
- [ ] **Adopt Zero Trust basics**: verify explicitly, use least privilege, assume breach. — WALK
- [ ] **Secure identities with managed identities** to avoid stored credentials. — WALK
- [ ] **Segment networks** with NSGs, private endpoints, and a firewall. — WALK
- [ ] **Enable diagnostic logging** and stream logs to a central Log Analytics workspace. — WALK
- [ ] **Pin data residency** to Canadian regions for Azure workloads. — WALK
- [ ] **Deploy Microsoft Sentinel** for cloud-scale SIEM, detection, and automated response. — RUN

06 Backup & recovery

RESILIENCE & RANSOMWARE READINESS

Assume something will fail. Backups you have actually tested are what get you back online.

- [ ] **Protect servers and VMs** with Azure Backup on a defined schedule. — CRAWL
- [ ] **Back up Microsoft 365 data** (mail, files, Teams) — the Microsoft SLA is not a backup. — CRAWL
- [ ] **Keep immutable / offline copies** so ransomware cannot encrypt your backups. — WALK
- [ ] **Enable Azure Site Recovery** for your most critical workloads. — WALK
- [ ] **Define RPO and RTO targets** for each critical system. — WALK
- [ ] **Test restores on a schedule** — an untested backup is a hope, not a plan. — RUN
- [ ] **Document and rehearse a recovery runbook** for a ransomware / outage scenario. — RUN

> **The 3-2-1 rule:** keep at least three copies of data, on two types of media, with one kept off-site or immutable. [add stat] of SMBs hit by ransomware had no tested restore.

07 Governance & monitoring

MICROSOFT SECURE SCORE & OPERATIONS

Security is a habit, not a project. Measure it, review it, and know who owns it.

- [ ] **Track and improve Microsoft Secure Score** — review the number every month. CRAWL
- [ ] **Assign a named owner** for security and privacy in your organization. CRAWL
- [ ] **Maintain an incident-response plan** with clear roles, steps, and contacts. WALK
- [ ] **Review user and privileged access** quarterly with access reviews. WALK
- [ ] **Centralize alerts and monitor sign-ins** for anomalies and impossible-travel. WALK
- [ ] **Keep an asset and data inventory** current so nothing is unmanaged. WALK
- [ ] **Run periodic security reviews** and tabletop exercises to stay sharp. RUN

Where to start: your Microsoft Secure Score is a single number that trends your progress — watch it climb as you work through this checklist.

Start here: your first five moves this week

- ✓ **Turn on MFA for everyone** and block legacy authentication.
- ✓ **Enrol devices** and require disk encryption on every machine.
- ✓ **Switch on** Safe Links, Safe Attachments, and anti-phishing.
- ✓ **Publish sensitivity labels** and keep Canadian data in-region.
- ✓ **Check your Microsoft Secure Score** and set a target to beat.

How VisioClara helps

YOUR MICROSOFT SECURITY PARTNER

We simplify Microsoft security for Canadian startups and SMBs — so you can make confident decisions and get more from the licences you already own. Vision-led on where you're headed, trust-built in how we protect your data, and clarity-driven in every recommendation we make.

✓ Security assessment
A clear read on your Microsoft Secure Score, gaps, and quick wins.

✓ Identity & device hardening
Entra ID, Conditional Access, Intune, and Defender, configured right.

✓ Data & compliance
Purview labels & DLP mapped to PIPEDA and Quebec Law 25.

✓ Azure Zero Trust
Defender for Cloud, Sentinel, and Canadian data residency by design.

✓ Backup & resilience
Azure Backup, Site Recovery, and tested ransomware readiness.

✓ Managed security
Ongoing monitoring, reviews, and a roadmap that keeps pace with growth.

Book a free discovery call or security review

30 minutes. We'll benchmark your Microsoft Secure Score, flag your top risks, and map a crawl / walk / run plan — PIPEDA and Law 25 included.

visioclara.com · info@visioclara.com · Toronto, Canada

Vision-led. Trust-built. Clarity-driven. — Microsoft, made simple.