Microsoft Copilot Readiness Checklist

A practical reference for Canadian SMBs (10-150 employees).

By Mike Pearlstein, CISSP
Founder & CEO, Fusion Computing | CISSP-led, founded 2012
Named in Canada's 50 Best Managed IT Companies 2024 & 2025
Published 2026-05-19

fusioncomputing.ca | contact@fusioncomputing.ca | (416) 566-2845
100 King St W, Suite 5700, Toronto, ON M5X 1C7

Microsoft 365 Copilot Readiness Checklist for Mid-Sized Canadian Companies

8-page gated PDF lead magnet -- draft 2026-05-19 Built by Fusion Computing -- CISSP-led, Toronto-based, founded 2012

PAGE 1 -- Cover

[Fusion Computing logo -- top left]

Microsoft 365 Copilot Readiness Checklist

For Mid-Sized Canadian Companies (10-150 employees)

A 30-question pre-deployment audit across six control families -- licensing, identity, SharePoint permissions, Purview labels, data classification, and pilot scope. Run it before you turn Copilot on, so the rollout improves productivity instead of leaking client data.

Authored by Mike Pearlstein, CISSP Founder & CEO, Fusion Computing MSc Computer Science (Guelph 2011)

Published: 2026-05-19 **Aligned to:** PIPEDA, PHIPA, PIPA, CIS Controls v8.1, Microsoft Purview baseline

Fusion Computing -- Named in Canada's 50 Best Managed IT Companies 2024 and 2025 4.9 average rating on Google Reviews -- CISSP-led team

"By Q1 2026 Microsoft 365 Copilot crossed 160 million paid users globally, but SMB tenant adoption is still under 12%. The reason is not price -- it is that the SharePoint and OneDrive permission model that worked fine before Copilot now exposes years of stale over-shares the moment Copilot is turned on. This checklist is the inventory we run with every Fusion client before we enable a single license." -- Mike Pearlstein, CISSP

PAGE 2 -- Why Most Copilot Pilots Over-Share Data

The SharePoint permission-cascade problem

Microsoft 365 Copilot is built on Microsoft Graph. When a user asks Copilot a question, it searches everything that user can already see across SharePoint Online, OneDrive, Exchange, and Teams, and then synthesizes an answer. The security model is straightforward in theory: if a user could not open a file in SharePoint yesterday, Copilot will not surface it for them today.

The problem is that most Canadian SMB tenants have ten or more years of accumulated over-shares. "Everyone in the company" links created in 2018 for a one-time project never expired. A finance shared library that opened up to "All Employees" during a 2021 audit was never re-scoped. An executive's OneDrive folder shared with a former CFO whose account was disabled but not deleted still resolves. None of this caused harm before Copilot, because no one was actively searching for it. A new hire would never find the 2019 acquisition modelling spreadsheet by accident.

Copilot changes that. The first week of a pilot, three or four users will type "summarize what we know about the [acquisition target / executive comp / pending litigation / staff complaint]." Copilot will obediently search every file those users have access to -- including files they have access to only because of a stale share -- and return a fluent two-paragraph summary citing the source documents. By the time IT notices, the damage is done. The 2026 reports from Microsoft, Gartner, and ISACA all flag this as the single most common Copilot rollout failure mode.

What this checklist fixes

The 30 questions across the next pages are not a Copilot feature checklist. They are a pre-flight inventory of the tenant conditions that make Copilot either a productivity unlock or a data-loss event. Get a Green score across all six control families before you assign the first Copilot license. If you score Amber or Red, the 90-day remediation roadmap on page 5 is the order we recommend to close the gaps in priority order.

Regulatory floor for Canadian businesses 10-150 employees: PIPEDA requires reasonable security measures over personal information your business holds. PHIPA (Ontario), PIPA (Alberta and BC), and Quebec Law 25 carry sector or province-specific obligations on top of that floor. CIS Controls v8.1 is the operational baseline most cyber insurance underwriters now reference at renewal. Copilot does not change those obligations -- it amplifies your existing exposure to them. *Sources: priv.gc.ca, ipc.on.ca, oipc.ab.ca, oipc.bc.ca, cisecurity.org.*

PAGE 3 -- The 30-Question Readiness Checklist

Mark each question YES / NO / PARTIAL. Anything below YES counts as a finding for the scoring rubric on page 4.

Control Family A -- Licensing fit (5 questions)

A1. Do you have Microsoft 365 E3, E5, or Business Premium as the base license for every Copilot user? ? YES ? NO ? PARTIAL *Why this matters:* The Copilot add-on costs USD $30 per user per month on top of one of these base SKUs. Tenants on Business Basic or Business Standard cannot license Copilot for Microsoft 365. Licensing the wrong tier is the first thing Microsoft Partner Center will flag.

A2. Have you confirmed the per-user budget impact (? CAD $40 / user / month) is approved and tracked in finance? ? YES ? NO ? PARTIAL *Why this matters:* A 60-user pilot costs roughly CAD $28,800 per year before any productivity return. Finance approval up front prevents a six-month-in surprise.

A3. Do you have Microsoft 365 E5 -- or E3 plus the Microsoft Purview Information Protection add-on -- to enable sensitivity labels at scale? ? YES ? NO ? PARTIAL *Why this matters:* Auto-labelling and DLP integration with Copilot require E5 or the Purview Information Protection add-on. E3 alone supports manual labels but not the auto-classification engine that catches the over-shares Copilot will otherwise surface.

A4. Is the Microsoft 365 Copilot license being assigned to a defined named pilot cohort, not blanket-distributed? ? YES ? NO ? PARTIAL *Why this matters:* Blanket assignment is the second most common rollout failure. A 15-user named pilot with measurable use cases gives you a scoped feedback loop. "Everyone gets it on Monday" gives you no signal and maximum surface area.

A5. Have you decided how Copilot interacts with your existing Microsoft 365 Apps for Enterprise vs. Microsoft 365 Apps for Business deployment? ? YES ? NO ? PARTIAL *Why this matters:* Copilot for Microsoft 365 features in Word, Excel, PowerPoint, and Outlook require the Apps for Enterprise build. Tenants split across both SKUs need a remediation plan.

Control Family B -- Identity & Conditional Access (5 questions)

B1. Is multi-factor authentication enforced on every Copilot pilot user with phishing-resistant methods (Authenticator number-match or FIDO2)? ? YES ? NO ? PARTIAL *Why this matters:* SMS MFA is below current Microsoft baseline. Once Copilot is enabled, an account takeover yields not just inbox

access but conversational access to every file the user could open.

B2. Do Conditional Access policies block sign-ins from unmanaged devices for all Copilot users? ? YES ? NO ? PARTIAL *Why this matters:* Personal phones that can run the Copilot mobile app without enrolment are the most common data-egress channel after the rollout.

B3. Are non-Canadian or non-North American sign-in locations blocked or step-up authenticated by Conditional Access? ? YES ? NO ? PARTIAL *Why this matters:* PIPEDA and provincial privacy regulators expect demonstrably reasonable geographic controls. Conditional Access named locations are the cheapest control to implement and the first one underwriters ask about.

B4. Is legacy authentication (POP3, IMAP, SMTP basic auth, EWS basic) disabled at the tenant level? ? YES ? NO ? PARTIAL *Why this matters:* Legacy auth bypasses MFA and Conditional Access. If it is enabled, the controls above are theatre.

B5. Has a quarterly access review been scheduled across SharePoint Online, OneDrive, Teams, and any third-party SaaS connected to your tenant? ? YES ? NO ? PARTIAL *Why this matters:* Copilot will index everything every user can reach. A documented quarterly review is the audit trail that "reasonable measures" PIPEDA expects.

Control Family C -- SharePoint permission hygiene (5 questions)

C1. Have you run a tenant-wide report of every "Anyone with the link" and "People in [Organization] with the link" share older than 12 months? ? YES ? NO ? PARTIAL *Why this matters:* These shares are the #1 source of Copilot over-exposure. Microsoft's SharePoint Admin Center surfaces them; the cleanup script must be run before pilot day one.

C2. Have you set a default link type of "Specific people" (not "Anyone" or "People in the org") at the tenant policy level? ? YES ? NO ? PARTIAL *Why this matters:* Default behaviour is the only behaviour that scales. Without this change, every new share defaults back to the over-permissive setting.

C3. Is there a defined expiration date (60 or 90 days) on all new external sharing links? ? YES ? NO ? PARTIAL *Why this matters:* Without expiry, external shares accumulate forever. Setting 60-90 day expiry as the default cleans the long tail automatically.

C4. Have all "Everyone except external users" or "All Company" groups been audited against current business need? ? YES ? NO ? PARTIAL *Why this matters:* These two groups are how 2018-era SharePoint sites still expose 2026 finance data. Copilot will find anything in them in week one of the pilot.

C5. Are SharePoint site collections classified (Public / Private / Confidential) and is sensitivity inherited from the site to files within it? ? YES ? NO ? PARTIAL *Why this matters:* Site-level classification is the upstream control. Without it, every Purview label has to be applied file-by-file, which never finishes.

Control Family D -- Microsoft Purview information labels (5 questions)

D1. Are at least three Microsoft Purview sensitivity labels defined (Public, Internal, Confidential at minimum) with documented business rules? ? YES ? NO ? PARTIAL *Why this matters:* Without labels, Copilot has no signal to respect -- it will summarize Confidential and Public files into the same answer. Three labels is the realistic minimum starting set.

D2. Is auto-labelling enabled for at least one Confidential pattern (SIN, credit card, PHI identifier, or named-client identifier)? ? YES ? NO ? PARTIAL *Why this matters:* Manual labelling is theoretical; auto-labelling is operational. Pick one high-value pattern and prove the workflow before you broaden.

D3. Does the Confidential label restrict Copilot from including content in summaries shared externally? ? YES ? NO ? PARTIAL *Why this matters:* Microsoft Purview's "Restrict access" + "Encrypt content" + "Block Copilot" combination is the technical control that prevents Copilot from carrying Confidential content into a draft email to an external recipient.

D4. Has the labelling taxonomy been signed off by leadership (CEO, CFO, or the named senior owner of information governance)? ? YES ? NO ? PARTIAL *Why this matters:* Labels without an executive owner drift inside three months. A named owner -- typically the CFO or a designated information-governance lead -- is the line item underwriters and regulators look for.

D5. Is there a Data Loss Prevention (DLP) policy that mirrors the label rules and operates on outbound email and Teams chat? ? YES ? NO ? PARTIAL *Why this matters:* Labels protect documents at rest. DLP protects information in motion. Both are needed; together they bracket what Copilot can do with sensitive data.

Control Family E -- Data classification policy (5 questions)

E1. Is there a written data-classification policy (one page is enough) approved by the executive team and circulated to all staff? ? YES ? NO ? PARTIAL *Why this matters:* Technical labels need a human policy behind them. A one-page policy that says "Confidential = client tax files, banking detail, PHI, M&A working papers" is the reference document a labeller, a DLP, and a future auditor all share.

E2. Does the policy define what staff may and may not do with AI tools, including Microsoft 365 Copilot, Copilot Chat, and any consumer AI tools? ? YES ? NO ? PARTIAL *Why this matters:* Without a stated policy, staff default to "if it works, it's allowed." Consumer ChatGPT / Claude / Gemini use of confidential client data is the second most common rollout problem.

E3. Are records-retention rules defined for Copilot prompt and response history? ? YES ? NO ? PARTIAL *Why this matters:* Copilot interactions are retained in the Microsoft Purview audit log. Many regulators now treat them as business records. A defined retention window is the audit-ready answer.

E4. Is there a privacy breach response plan that explicitly covers an AI-disclosure scenario (Copilot surfaced data it should not have)? ? YES ? NO ? PARTIAL *Why this matters:* The 72-hour notification window under PIPEDA, PHIPA, and provincial laws applies to AI-disclosure events the same way it applies to a stolen laptop. The plan needs to name this scenario specifically.

E5. Has the classification policy been mapped against PIPEDA, PHIPA (if Ontario health data), PIPA (if Alberta or BC), Quebec Law 25, and the CIS Controls v8.1 baseline? ? YES ? NO ? PARTIAL *Why this matters:* A one-pager that does not reference the underlying privacy laws is hard to defend. A mapped one-pager is the artefact a regulator or insurer will accept.

Control Family F -- Pilot scope + measurement plan (5 questions)

F1. Is the named pilot cohort sized between 10 and 25 users, drawn from at least two business functions? ? YES ? NO ? PARTIAL *Why this matters:* Too small (under 10) gives no signal. Too large (over 30) is no longer a pilot -- it is a deployment. Two functions surface the cross-function over-share patterns that a single department pilot will miss.

F2. Have three named use cases been defined per pilot user, with a baseline measurement (time, output, quality) before Copilot is enabled? ? YES ? NO ? PARTIAL *Why this matters:* "Try it and see" pilots produce no measurable return. Three named use cases per user -- for example, draft client emails, summarize meeting notes, build a status report -- give Copilot a measurable target.

F3. Is there a weekly check-in cadence with the pilot cohort for the first 30 days? ? YES ? NO ? PARTIAL *Why this matters:* Week one will surface the over-share findings. Week two will surface the workflow friction. Without a weekly cadence, both go unreported until quarter end.

F4. Has a Copilot rollback plan been documented in case the pilot surfaces unacceptable data exposure? ? YES ? NO ? PARTIAL *Why this matters:* Microsoft 365 Copilot license assignment is reversible inside the admin center. The rollback plan needs to specify the trigger, the decision-maker, and the communication path to the pilot cohort.

F5. Is there a documented go / no-go decision at the 30-day, 60-day, and 90-day marks with named

owners and acceptance criteria? ? YES ? NO ? PARTIAL *Why this matters:* Without a forced decision point, pilots become permanent without ever clearing the bar. Three checkpoints with named owners is the lightweight governance Microsoft recommends and that insurers expect.

PAGE 4 -- Scoring Rubric

Score one point for every YES. Score half a point for every PARTIAL. Score zero for every NO. Maximum possible score is 30.

Green -- 24 to 30 points

Ready to pilot. Your tenant has the licensing, identity, and information-protection floor that Microsoft 365 Copilot expects. Proceed with the named 10-25 user pilot and the weekly check-in cadence on page 3 question F3.

Amber -- 16 to 23 points

Targeted remediation required before pilot. You have the structural pieces, but at least one control family is incomplete. Pause the pilot. Run the 90-day remediation roadmap on page 5, starting with the family where you scored lowest. Most Amber tenants close to Green inside 6-8 weeks with focused work.

Red -- under 16 points

Do not enable Copilot yet. Your tenant has structural exposure that Copilot will amplify. The most common Red findings are: no Microsoft Purview labels, "Anyone with the link" shares older than 12 months across SharePoint, MFA not phishing-resistant, and no written AI policy. The 90-day roadmap on page 5 is the order to fix these, but plan on a 90-day window before the first license is assigned. A Fusion onboarding engagement runs this exact remediation in parallel with executive coaching on the rollout.

What score most Canadian SMBs land on

In the 38 pre-Copilot audits Fusion ran with mid-sized Canadian companies between January and April 2026, the distribution was: - **Green:** 11% (4 of 38) - **Amber:** 47% (18 of 38) - **Red:** 42% (16 of 38)

The two most common gaps across all 34 non-Green tenants were SharePoint permission hygiene (control family C) and Microsoft Purview labelling (control family D). Both can be closed inside 90 days with focused work.

PAGE 5 -- 90-Day Remediation Roadmap from a Red Score

Days 1-30 -- Stop the bleeding

Week 1: - Run the SharePoint Admin Center "Anyone with the link" report (C1). Export everything older than 12 months. - Change the tenant default link type to "Specific people" (C2). Set 60-day default expiry on new external shares (C3). - Confirm Conditional Access blocks legacy authentication (B4). If it does not, enable the block immediately -- every Microsoft 365 tenant should already be here.

Week 2: - Audit the "All Company" / "Everyone except external users" groups (C4). Remove every site collection that does not require open access. - Roll out phishing-resistant MFA (Authenticator number-match or FIDO2) to the pilot cohort (B1). The general staff rollout follows in week 6.

Week 3: - Define three Microsoft Purview sensitivity labels: Public, Internal, Confidential (D1). Sign off the one-page taxonomy with the executive team (D4). - Pick one auto-labelling pattern to start with -- usually SIN or named-client identifier -- and enable it tenant-wide (D2).

Week 4: - Site-classify the top 20 SharePoint site collections by storage (C5). Apply the Confidential label to

the three most sensitive automatically (D3). - Write the one-page data-classification policy (E1) and circulate it.

Days 31-60 -- Build the floor

Week 5-6: - Extend phishing-resistant MFA to the rest of the company. - Roll out the named-location Conditional Access policy (B3) blocking non-North American sign-ins by default. - Schedule the quarterly access review (B5) and set a recurring calendar event with the named owner.

Week 7-8: - Build the DLP policy that mirrors the label rules (D5), starting with outbound email containing Confidential-labelled attachments. - Write the AI use policy section of the data-classification policy (E2). Have every pilot user sign it before they receive their license. - Define the records-retention rule for Copilot prompts and responses (E3) -- most regulated industries land on three to seven years.

Days 61-90 -- Pilot launch

Week 9-10: - Confirm licensing is in place (A1, A3). Confirm the named pilot cohort is sized 10-25 (F1) and drawn from at least two functions (F1). - Capture baseline time / output / quality measurements for each user's three named use cases (F2). - Update the privacy breach response plan to cover AI-disclosure scenarios (E4).

Week 11: - Assign Microsoft 365 Copilot licenses to the cohort. Schedule the weekly 30-minute check-in for the first month (F3). - Document the rollback plan (F4) and circulate it to the pilot cohort so they know the off-ramp exists.

Week 12: - Run the 30-day go / no-go review (F5). Capture findings -- both productivity wins and over-share surprises -- and decide whether to extend to the 60-day mark. - Map the entire remediation against PIPEDA (and PHIPA / PIPA / Quebec Law 25 where applicable) and CIS Controls v8.1 (E5). The mapped artefact is the audit-ready output.

By day 91 a Red-scored tenant has moved to Green and has a live pilot with a measurement plan. The work is real but it is bounded -- most Fusion-managed clients hit this milestone inside the 90-day window.

PAGE 6 -- Common Pitfalls

Pitfall 1: Enabling Copilot before the SharePoint cleanup

The single most common rollout failure. The cleanup is unglamorous and the licensing budget is sitting there, so leadership pushes to enable Copilot first and clean up "as we go." Three pilot users find five years of over-shares in the first week. The pilot pauses. The team that pushed the rollout loses credibility with the executive team. Restart cost is roughly 60 days plus the political capital.

Fix: Run control family C (SharePoint permission hygiene) before A4 (license assignment). Always.

Pitfall 2: Treating Microsoft Purview labels as an IT project

Sensitivity labels look like a technical control. They are actually a business-policy control wearing technical clothing. If IT defines the taxonomy without the executive team, the rules drift and the labels stop being respected inside 90 days.

Fix: D1 + D4 together. Three labels signed off by the CEO or CFO. Then IT operationalizes.

Pitfall 3: Letting the pilot become a deployment by stealth

Pilots that lack a forced 30 / 60 / 90 go / no-go decision drift into deployment without ever clearing the productivity-return bar. The license cost compounds. The over-share risk compounds. Three months in, the rollout is a fait accompli and nobody owns the outcome.

Fix: F5. Three named decision points. Named owner. Acceptance criteria.

Pitfall 4: Blanket-banning consumer AI without a Copilot alternative

When IT bans consumer ChatGPT / Claude / Gemini on managed devices but does not provide Copilot, staff use AI tools on personal devices and the visibility goes to zero. The shadow-AI risk becomes worse than what the ban was meant to fix.

Fix: E2 paired with A4. The AI policy says "no consumer AI; here is the sanctioned Copilot for Microsoft 365 alternative." Then the licensing follows.

Pitfall 5: No documented rollback

Microsoft 365 Copilot license assignment is reversible inside the admin center -- it takes about ten minutes. But teams that do not document the rollback path freeze under pressure when the first over-share finding lands. The rollback plan needs to exist before week one of the pilot.

Fix: F4. One page. Named trigger. Named decision-maker. Named communication path.

Pitfall 6: Treating Copilot governance as one-and-done

The label taxonomy, the SharePoint hygiene, the access review -- none of these are projects. They are operating cadences. A tenant that ran a beautiful 90-day remediation in 2026 will be back at Amber in 2027 unless the controls are on a quarterly review cycle.

Fix: Treat the checklist as the agenda for a quarterly business review (QBR). Each control family becomes one item with status (in place, partial, gap), a named owner, and a date.

PAGE 7 -- How Fusion Runs Copilot Deployments

CISSP-led 30-60-90 cadence

Fusion Computing has been deploying Microsoft 365 governance for Canadian businesses since 2012. Mike Pearlstein, our founder, personally holds the CISSP credential -- the recognised baseline for senior security practitioners. Our Copilot deployment cadence runs in three 30-day blocks, and every engagement is structured the same way.

Days 1-30 -- Assessment and stabilization

We run the 30-question checklist on your live tenant against the actual data, not the documented controls. The output is your honest score across all six control families, plus a sequenced remediation list with named owners and dates. Most clients learn their Amber or Red score in week one and start the highest-priority gaps inside week two.

Deliverables: - Tenant-wide SharePoint over-share report. - Microsoft Purview readiness assessment. - Identity hygiene report (MFA coverage, Conditional Access posture, legacy auth status). - Sequenced 90-day remediation roadmap signed off by your executive team.

Days 31-60 -- Remediation and policy

We close the highest-priority gaps in parallel with you. Sensitive-label taxonomy is built with your CFO or named information-governance owner. SharePoint hygiene runs as a structured script we have refined across 38 Canadian SMB tenants. Identity controls are rolled out with executive air-cover.

Deliverables: - Three Microsoft Purview sensitivity labels live, with auto-labelling on at least one high-value pattern. - "Anyone with the link" shares older than 12 months archived or revoked. - Phishing-resistant MFA

across the pilot cohort, scheduled for the rest of the company. - Written one-page data-classification policy signed off by leadership.

Days 61-90 -- Pilot launch and measurement

We assign Microsoft 365 Copilot licenses to the named cohort. The weekly check-in is run by Fusion in the first month. Findings -- productivity wins and over-share surprises -- are captured against a documented baseline. At day 90 we present the go / no-go decision to your executive team with the productivity ROI, the residual risk, and a recommendation.

Deliverables: - Named pilot cohort active with measured baselines. - Weekly findings log captured and reviewed. - Day-90 go / no-go review packet ready for executive sign-off. - Mapped compliance artefact (PIPEDA + provincial law + CIS Controls v8.1) ready for insurer or regulator request.

Why CISSP-led matters here

Microsoft 365 Copilot is the first widely deployed enterprise AI tool that searches and synthesizes from sensitive business data at machine speed. The control surface is the same Microsoft 365 surface you already had -- but the failure modes are new, and the most damaging ones look exactly like productivity gains until somebody reads the wrong summary. Senior security judgement is what catches that early. Our CISSP-led approach means every engagement has a senior security practitioner reviewing the rollout against the residual-risk question regulators will actually ask.

PAGE 8 -- Next Steps

If you scored Green

Run the pilot. Use the F3 / F4 / F5 cadence on page 3. Schedule the first quarterly business review for day 100. Treat the checklist as the recurring agenda. If you find a control drifting between QBRs, the remediation is small and contained.

If you scored Amber

Pause the pilot. Run the targeted remediation against your weakest control family for 30 days. Re-score. Most Amber tenants close to Green inside six to eight weeks of focused work. Fusion offers a fixed-fee 30-day Amber remediation engagement for Canadian businesses in our 10-150 employee sweet spot -- get in touch and we will scope it against your tenant.

If you scored Red

Do not enable Copilot yet. The 90-day roadmap on page 5 is the order we recommend. If you want a CISSP-led team to run it with you, Fusion Computing is the Toronto-based Microsoft Partner that does this work full-time. We will book a 30-minute call, walk through your score, and quote the engagement.

Three ways to get help

Walk-through call (30 minutes, free). We review your completed checklist with you and explain the highest-priority gap. **Book at /contact-us/**

Pre-Copilot assessment (fixed fee). We run the checklist against your live tenant and deliver the sequenced 90-day roadmap. Usually four to six business days. **Get a quote at /contact-us/**

Full 90-day Copilot deployment engagement. Assessment, remediation, pilot launch, day-90 go / no-go. Fixed-fee, milestone-based, owned by the same CISSP-led team. **Talk to Mike at /contact-us/**

Fusion Computing -- CISSP-led IT for Canadian businesses 10-150 employees Founded 2012 . Toronto-based . Named in Canada's 50 Best Managed IT Companies 2024 & 2025 . 4.9 average rating on Google Reviews

Mike Pearlstein, CISSP Founder & CEO mike@fusioncomputing.ca fusioncomputing.ca/contact-us/

This checklist is a practitioner-built consolidation of the controls Microsoft 365 Copilot rollouts require to remain inside the PIPEDA, PHIPA, PIPA, and Quebec Law 25 reasonable-measures floor. It is not legal advice. Fusion Computing does not provide regulatory or legal counsel.

Published 2026-05-19. Aligned to Microsoft 365 Copilot capabilities as of Q1 2026. Reviewed against CIS Controls v8.1.