NORTHSECURE AI

The Canadian SMB AI Readiness Checklist

A practical guide to workplace AI governance, security, and compliance readiness.

READINESS DISCIPLINARY AUDIT

01. AI Usage Visibility & 02. Data & Privacy

01. AI USAGE VISIBILITY

- [ ] **Approved AI Tools Defined**
  We have a clear, formally documented list of corporate-approved AI applications and platforms.
- [ ] **Leadership Visibility**
  Executive teams and department heads have clear insight into how and where AI is utilized within operations.
- [ ] **Shadow AI Strategy**
  We actively monitor or have addressed "Shadow AI" (unauthorized use of personal accounts or tools by staff).
- [ ] **AI Vendor Inventory**
  All production software vendors embedded with generative AI capabilities have been explicitly cataloged.
- [ ] **Data-Use Terms Understood**
  We have verified whether our everyday tools use company inputs to train public generative models.

02. DATA & PRIVACY

- [ ] **Confidentiality Rules Established**
  Specific rules exist detailing what tier of information is legally allowed inside artificial intelligence prompts.
- [ ] **Public AI Tool Controls**
  Technical or strict behavioral controls prevent corporate IP or source code from entering consumer-grade public models.
- [ ] **Data Classification Sync**
  Our data classification scheme aligns cleanly with access controls configured inside AI tools like Microsoft Copilot.
- [ ] **Privacy Mandate Review**
  We have reviewed customer, provincial, and federal privacy obligations (e.g., PIPEDA) regarding AI data storage.

READINESS DISCIPLINARY AUDIT

03. Governance & 04. Technical Security

03. GOVERNANCE

- [ ] **Assigned AI Ownership**
  A designated internal lead, executive, or external advisor explicitly owns AI security and alignment strategy.
- [ ] **Acceptable Use Standards**
  Clear expectations are published concerning fair, unbiased, and mathematically accurate application of AI outputs.
- [ ] **Documented Risk Profile**
  Legal, financial, operational, and reputational exposures tied to AI adoption are logged and reviewed.
- [ ] **Incident Escalation Paths**
  We possess a clear response structure if an AI data leak, model poisoning, or API abuse occurs.

04. TECHNICAL SECURITY

- [ ] **Multi-Factor Authentication (MFA)**
  Enforced across all standalone enterprise AI licenses, portals, API access panels, and administration nodes.
- [ ] **Role-Based Access Controls (RBAC)**
  AI tools respect internal data isolation boundaries; an employee cannot access unauthorized files via prompt queries.
- [ ] **Third-Party AI Evaluation**
  Any integrated third-party AI plug-in or API browser extension goes through formal IT security vetting before deploy.
- [ ] **AI Security Awareness Training**
  Employees receive explicit education regarding AI-driven phishing threats, deepfakes, and safe prompt techniques.

READINESS DISCIPLINARY AUDIT

05. Policy Realism & 06. Vendor Compliance

05. POLICY REALISM

- [ ] **Acceptable Use Policy (AUP) Integration**
  We have updated or created a standalone, easily read policy defining authorized AI behavior across teams.
- [ ] **Continuous Communication Plan**
  The approved tools list is regularly highlighted to employees so shadow software adoption drops.
- [ ] **Mandatory Output Validation**
  Processes dictate that AI-generated artifacts (code, copy, designs, reports) undergo human review for errors/hallucinations.
- [ ] **Functional Guardrails Defined**
  HR, legal, and accounting teams possess specialized instructions tailored to their sensitive document parameters.

06. VENDOR & COMPLIANCE

- [ ] **Articulate AI Strategy to Clients**
  Sales, account management, and leadership teams can clearly explain our company's approach to secure AI to clients.
- [ ] **Prepared for Questionnaires**
  We possess standard, compliant answers for inbound enterprise enterprise vendor risk assessment questionnaires.
- [ ] **Vendor Due Diligence Upgrades**
  Our onboarding assessments evaluate how incoming contractors and suppliers protect our shared files from AI models.
- [ ] **Proactive Regulatory Preparation**
  Our framework looks ahead toward upcoming Canadian AI legal changes, avoiding expensive compliance retrofitting.

EVALUATION DASHBOARD

AI Readiness Scorecard

Total up your marked checkboxes from sections 1 through 6 (25 criteria total) to locate your company's governance tier below:

24-25	15-23	< 15
OPTIMIZED	PROGRESSIVE	EXPOSED

24–25 CHECKS

Strong Foundation

Your organization has a highly mature framework. Continue monitoring software shifts and maintaining active employee communication.

15–23 CHECKS

Good Progress

Solid structural components exist, but significant governance, technical permission visibility, or control gaps require active resolution.

UNDER 15

High AI Exposure

AI tools are moving faster than your governance and security structures can secure them. Immediate baseline guidelines are strongly recommended.

Need help resolving gaps found in your evaluation? Turn the page for immediate tactical assistance.

Want a practical review?

Deploy operational AI safely. NorthSecure AI helps Canadian mid-market firms and small businesses confidently structure governance, protect sensitive assets, and handle enterprise security audits cleanly.

- ✓ Adopt workplace AI tools with absolute confidence
- ✓ Uncover and remedy governance, access, and security vulnerabilities
- ✓ Build highly practical, realistic policies and operational guardrails
- ✓ Prepare seamlessly for security audits and customer compliance demands

Free AI & Security Readiness Consultation

15 MINUTES	NO SALES DECK	NO BUZZWORDS	PRACTICAL ADVICE

Web: northsecure.ai | **Email:** info@northsecure.ai

Scan below or reach out directly via your browser to secure an opening on our advisory calendar.