

THE AI ADVANTAGE SERIES

Security essentials for leaders in the AI age

A program of The AI Leveraged Leader and Elliptic Systems Corporation



CANADIAN EDITION

The Security Starter Toolkit

Six documents to build your company's security plan in an afternoon

Why this toolkit exists

If you provide a product or a service to anyone, you now have a duty of care for their security while they use it. Most owners we meet do not need more warnings. They need a starting point that fits a company their size, and a way to know they are on track without becoming a security expert themselves. That is what this packet is for.

What it gives you

Six working documents, each one customizable for your company in minutes: a way to classify what data can go into an AI tool, a usage policy you can put your name on, the five decisions a leadership team has to make and record, a scorecard for judging vendors before you hand them your customers' data, a twenty-minute weekly checklist that lets a leader sleep at night, and a wall card that says who to call and what to do in the first thirty minutes of an incident. This Canadian edition rewrites every document for a company with a U.S. office, a Canadian office, or customers in both. The rules that are the same on both sides of the border are stated once; where they differ, a marked box gives the Canadian rule (PIPEDA, BC and Alberta PIPA, Quebec Law 25, Bill C-8, CyberSecure Canada) and the U.S. rule (state privacy and breach laws, HIPAA, GLBA, CMMC, SEC) side by side, with the regulators and agencies to call in each country.

How to use it

Read the five decisions worksheet first, then work through the others in the order listed. Block a few hours, get your key people in the room, and fill in the blanks. None of it requires a security team. It requires a leader who decides that customer safety is part of running the business.

Companion download: the Vendor Evaluation Scorecard is also provided as a working Excel spreadsheet (Canadian edition) with the weighting formulas built in. Download it separately alongside this PDF.

Please read. This toolkit is educational material, not legal advice. Laws, regulator guidance and the AI and security landscape are changing quickly, and we expect the Canadian terms in these documents to change too. Confirm current requirements with your legal advisor, the Office of the Privacy Commissioner of Canada (priv.gc.ca), your provincial commissioner, and the Canadian Centre for Cyber Security (cyber.gc.ca) before you rely on any of it. Content current to September 2026.



The AI Leveraged Leader

Leanne Terrace

AI strategist, executive coach,
author of Built to Think

linkedin.com/in/leanneterrace
leanne@leanneterrace.com



Elliptic Systems Corporation

Eric Stefanik

CEO, cybersecurity and AI governance; Secure AI Academy
linkedin.com/in/ellipticsystems
eric@ellipticsystems.com

Contents

Canadian Edition: U.S. and Canadian requirements integrated in every document. Not legal advice; current to September 2026 and subject to change.

- | | | |
|--|--|----------------|
| 01 | AI Data Classification Template | page 3 |
| Four tiers, examples by industry, a decision tree, and the U.S. and Canadian identifiers and de-identification standards side by side. | | |
| <hr/> | | |
| 02 | AI Usage Policy (fill-in template) | page 13 |
| Eighteen sections plus regulator contacts: approved tools, acceptable use, privacy law in both countries, vendor terms, monitoring notice, incident reporting duties. Add your name and your tools. | | |
| <hr/> | | |
| 03 | The 5 Critical Infrastructure Decisions | page 24 |
| The five calls a leadership team has to make and write down, with cross-border data residency and the certification checklist for both countries. | | |
| <hr/> | | |
| 04 | Security Vendor Evaluation Scorecard | page 32 |
| A weighted score for any tool on adoption, fit, support, real cost (in either currency) and security, with a certification checklist for both countries. The working spreadsheet is a separate download. | | |
| <hr/> | | |
| 05 | Daily Defense Checklist, Leadership Edition | page 36 |
| Eight questions, twenty minutes a week, with the compliance checkpoint written for both countries. How a leader stays confident without reading logs. | | |
| <hr/> | | |
| 06 | When to Escalate: Urgency Levels | page 39 |
| Green, yellow, orange, red. What counts as an incident, the first three steps, and a fourth step: who to report to in Canada and in the United States, and by when. | | |
| <hr/> | | |

Companion download

04 - Vendor Evaluation Scorecard (Canadian edition).xlsx: the working spreadsheet with weighted scoring formulas. Use it alongside document 04 when you evaluate a vendor.



AI DATA CLASSIFICATION TEMPLATE

Clear Guidelines for Safe AI Adoption, United States and Canada

By Elliptic Systems Corporation

(Protecting What Matters While Enabling Innovation)

PURPOSE OF THIS TEMPLATE

This classification system helps employees quickly determine what data can safely be used with AI tools. The four-tier system balances innovation with protection, and it works the same way whether your office, your employee or your customer is in the United States or in Canada. Where the law uses a different name or sets a different rule on each side of the border, this template says so in a marked box.

Remember: When in doubt, classify UP (more restrictive). It is easier to relax restrictions than to recover from a breach.

BOTH COUNTRIES

Personal information is the common thread. In Canada, PIPEDA and the provincial privacy laws (BC PIPA, Alberta PIPA, Quebec Law 25) treat any information about an identifiable individual as personal information. In the United States there is no single federal privacy law; state laws (California CCPA/CPRA, Virginia, Colorado, Texas and others) and sector laws (HIPAA, GLBA, FERPA) apply instead. For AI use the practical rule is the same in both countries: a record that identifies a customer, employee or contact is at least Tier 3 until it has been de-identified.

THE FOUR-TIER SYSTEM

TIER 1: PUBLIC DATA (Green)

Safe for ANY AI tool (consumer or enterprise)

Definition: Information already publicly available or intended for public release with no competitive, legal, or privacy concerns.

AI Tool Usage: No restrictions

Public data examples (universal):

- Published marketing materials, press releases
- Public website content
- General industry research and news articles
- Published financial statements (for public companies)
- Job postings and company overview information
- Conference presentations already delivered
- Social media content already posted

Industry-specific public data examples:

Industry	Examples
Legal firms	Published case law and court decisions; firm bios and practice descriptions; published blog posts and articles; post-event speaking materials
Construction	Completed project photos (with client approval); general safety procedures and standards; capability statements; award announcements
Healthcare	Properly de-identified research data; general health education materials; published clinical trial results; facility information and services



Industry	Examples
Finance	Public market analysis and industry reports; investment education materials; public regulatory guidance; published economic forecasts
Architecture	Portfolio projects (with client permission); design philosophy statements; sustainability certifications; award-winning project showcases
Manufacturing	Public product catalogs and specifications; safety data sheets; general capabilities; quality certifications achieved

TIER 2: INTERNAL DATA (Yellow)

Company information requiring **APPROVED ENTERPRISE AI tools only**

Definition: Internal business information that is not confidential but should remain within the organization and trusted partners.

AI Tool Usage: Enterprise AI tools with data processing agreements (DPAs) only

Required controls:

- Use only the company-approved AI tool stack
- Do not use consumer AI accounts
- Company data stays within the enterprise environment

Internal data examples (universal):

- Internal meeting notes and agendas
- Employee directory and organizational charts
- Project plans and timelines (non-confidential)
- Internal training materials
- Company policies and procedures
- General budget discussions (not specific figures)
- Team collaboration documents
- Non-confidential email correspondence

Industry-specific internal data examples:

Industry	Examples
Legal firms	Matter management and case tracking; internal regulatory training; firm strategic planning; non-privileged client communications; internal research memos
Construction	Project schedules and milestones; internal safety training; subcontractor coordination; equipment inventory and maintenance logs; pre-submission bid worksheets
Healthcare	Staff scheduling; internal compliance training; quality improvement initiatives; supply inventory and ordering; facility maintenance schedules
Finance	Internal analysis and research notes; portfolio management workflows; compliance procedures; regulatory staff training; internal performance metrics
Architecture	Early concept sketches; internal design reviews; resource allocation planning; software and tool standards; professional development plans
Manufacturing	Production schedules; equipment maintenance procedures; inventory data; quality control checklists; employee training modules

TIER 3: CONFIDENTIAL DATA (Orange)

Client data, financials: **RESTRICTED AI use with specific controls**



Definition: Sensitive business information that could cause significant harm if disclosed, including client data, financial details, and competitive intelligence.

AI Tool Usage: Restricted. Requires data sanitization plus department head approval.

Required controls:

- Data must be sanitized or anonymized before AI input
- Remove identifying information (names, numbers, specifics)
- Document AI usage and purpose
- Use only enterprise AI tools with explicit DPAs
- Activity logging and audit trail enabled
- Department head or designated approver signs off

CANADA

Quebec customers and employees. Under Law 25, personal information about a Quebec resident that will leave Quebec (including to a U.S.-hosted AI tool) requires a documented privacy impact assessment before the transfer. Treat Quebec personal information as Tier 3 with that added step, and name who completes the assessment.

UNITED STATES

State privacy laws. If you hold data on residents of California, Colorado, Connecticut, Texas, Virginia or another state with a comprehensive privacy law, "sensitive personal information" (precise location, biometric, health, financial account, immigration status, data of children under 13) generally needs opt-in consent before processing and belongs in Tier 4, not Tier 3.

Confidential data examples (universal):

- Client/customer lists and contact information
- Pricing strategies and discount structures
- Financial statements and P&L details
- Employee compensation and benefits data
- Contract terms and negotiations
- Strategic business plans
- Competitive analysis and intelligence
- Merger and acquisition discussions (pre-announcement)
- Proprietary methodologies and processes
- Vendor agreements and pricing

Industry-specific confidential data examples:

Industry	Examples
Legal firms	Client matter details and case strategies; billing rates and fee arrangements; conflict check information; client confidences and work product; settlement negotiations; witness lists and evidence inventories
Construction	Detailed project budgets and costs; bid pricing and margins; client contracts and change orders; subcontractor pricing; project-specific safety plans; proprietary construction methods
Healthcare	Patient health information (US: PHI under HIPAA; Canada: personal health information under PHIPA, PIPA, HIA and equivalents); insurance and billing details; clinical outcomes data before de-identification; credentialing information; quality metrics and incident reports; vendor contracts



Industry	Examples
Finance	Client account information and holdings; investment strategies and recommendations; transaction details and trade history; risk assessments and credit analyses; regulatory examination findings; client financial plans
Architecture	Client project details and requirements; detailed specifications and drawings; project budgets and fee proposals; proprietary design techniques; client communications; site analysis and feasibility studies
Manufacturing	Customer order details and specifications; supplier contracts and pricing; production costs and margins; client-specific quality data; proprietary processes and formulas; supply chain relationships

TIER 4: RESTRICTED DATA (Red)

Trade secrets, legal privilege: NO AI without EXECUTIVE approval

Definition: Highest-sensitivity data where disclosure could cause severe damage, including trade secrets, legal privilege, and regulated data requiring special protection.

AI Tool Usage: Prohibited without explicit C-suite or executive approval

Required controls:

- Executive approval required (CEO, CFO, General Counsel, or designated executive)
- Written justification for AI usage
- Maximum security controls applied
- May require an air-gapped or specialized secure environment
- Legal review if applicable
- Complete audit trail maintained

BOTH COUNTRIES

Government identifiers are always Tier 4. United States: Social Security numbers, driver's licence numbers, passport numbers. Canada: Social Insurance Numbers (SIN), provincial health card numbers, driver's licence numbers, passport numbers. None of these should ever be entered into an AI tool.

Restricted data examples (universal):

- Trade secrets and proprietary IP
- M&A due diligence and negotiations (pre-announcement)
- Attorney-client (Canada: solicitor-client) privileged communications
- Regulatory investigation materials
- Pending litigation strategy and documents
- Proprietary source code and algorithms
- Board meeting materials and minutes
- Executive compensation details
- Planned major business transactions
- Whistleblower complaints and investigations

Industry-specific restricted data examples:

Industry	Examples
Legal firms	Privileged communications; work product and trial strategy; grand jury materials (US); sealed court documents; client confidences under ethics rules; conflict of interest information



Industry	Examples
Construction	Proprietary techniques and patents; major incident investigation files; regulatory violation investigations (OSHA in the US; WorkSafeBC, Alberta OHS and other provincial regulators in Canada); litigation and claims files; trade secret equipment designs
Healthcare	Sensitive health information (HIV status, mental health, substance use); pre-approval research data; peer review and credentialing decisions; privileged incident reports; breach investigations (HIPAA in the US; provincial health privacy law in Canada); controlled substance records
Finance	Insider trading watch lists; regulatory examination work papers; suspicious activity or transaction reports (FinCEN SARs in the US; FINTRAC STRs in Canada); client government identifiers and account numbers; proprietary trading algorithms; material non-public information
Architecture	Patented or patent-pending innovations; security and life-safety system designs; classified or protected government facility designs; proprietary structural calculations; identified client security vulnerabilities
Manufacturing	Trade secret formulations; proprietary processes; pending patents; unresolved product defect investigations; compliance issues under investigation; reverse-engineered competitor analysis



DECISION TREE: "WHICH TIER IS MY DATA?"

Start here and answer the questions in order.

Question 1: Is this data already public or intended for public use?

- YES: PUBLIC (Tier 1). Safe for any AI tool.
- NO: Continue to Question 2.

Question 2: Does this data include any of the following?

- Trade secrets or proprietary IP
- Attorney-client or solicitor-client privilege
- Pending litigation or regulatory investigation
- M&A or major business transactions (pre-announcement)
- Board-level confidential materials
- Regulated sensitive data (US: SSN, financial account numbers, HIPAA PHI; Canada: SIN, health card numbers, personal health information)
- YES: RESTRICTED (Tier 4). Executive approval required.
- NO: Continue to Question 3.

Question 3: Does this data include client or customer information, financials, or competitive intelligence?

- YES: CONFIDENTIAL (Tier 3). Sanitize plus approval required.
- NO: Continue to Question 4.

Question 4: Is this internal company information not intended for public release?

- YES: INTERNAL (Tier 2). Enterprise AI tools only.
- NO: Return to Question 1 (likely PUBLIC).

DATA SANITIZATION GUIDE

How to make Confidential data safe for AI. When you have Tier 3 data that you need AI help with, sanitize it first.

Remove or generalize:

1. Personal identifiers

- Names: "Client A," "Customer 1," "Employee X"
- Email addresses: "contact@example.com" or remove entirely
- Phone numbers: "XXX-XXX-XXXX" or remove
- Addresses: "City, State" or "City, Province" only, or "West Coast location"

2. Financial specifics

- Exact figures: round to ranges ("50-75K" instead of "\$67,342")
- Account numbers: "Account ending in 1234"
- Pricing: "Industry-standard pricing" or percentage ranges

3. Dates and times

- Specific dates: "Q2 2026" or "Late spring"
- Recent events: "Within the last month"

4. Company and client names

- Company names: "Large regional bank," "Fortune 500 tech company"
- Competitor names: "Competitor A," "Major competitor"



CANADA

What "de-identified" has to mean in Canada. The Office of the Privacy Commissioner treats information as de-identified only when there is no serious possibility of re-identifying a person, alone or combined with other data. Removing a name is not enough if the record still holds a postal code, birth date, employer and job title together. Remove or generalize all of them.

UNITED STATES

What "de-identified" has to mean in the United States. HIPAA's Safe Harbor standard lists 18 identifiers that must be removed (names, dates more specific than year, ZIP codes beyond the first three digits, contact details, government and account numbers, biometrics, photos). State privacy laws use a similar "reasonably linkable" test. Use the HIPAA list as your checklist even outside healthcare; it is the most complete one available.

Example sanitization

BEFORE (Confidential, do not use in AI): "John Smith at Acme Corp (john.smith@acme.com) requested a bid for \$125,000 on the Seattle project scheduled for March 15, 2026. This undercuts our competitor BuildCo's \$140,000 quote."

AFTER (Sanitized, OK for AI with approval): "A client in the Pacific Northwest requested a bid in the \$100-150K range for a mid-sized commercial project in Q1 2026. Our pricing is approximately 10% below a major competitor's quote."

FREQUENTLY ASKED QUESTIONS

Q: What if I am not sure which tier my data falls into?

A: Classify UP (more restrictive). Better to be overly cautious and get approval than to under-protect sensitive data. When in doubt, ask your manager or IT/Security team.

Q: Can I use ChatGPT or Claude for Tier 2 (Internal) data?

A: Only if you are using the ENTERPRISE versions with a company account and a data processing agreement. Consumer accounts (free or personal subscriptions) should only be used for Tier 1 (Public) data.

Q: What happens if I accidentally upload Confidential data to a consumer AI tool?

A: Report it immediately to IT/Security and your manager. Quick response can minimize damage. Do not delete the conversation; we may need it for investigation. You will not be punished for honest mistakes reported promptly.

Q: How do I know which AI tools are "approved enterprise tools"?

A: Check with IT or reference the company's Approved AI Tool Stack document. If a tool is not on the list, request evaluation before using it with Internal, Confidential, or Restricted data.

Q: Can I use AI to help write emails that contain client information?

A: Yes, if you sanitize the data first (remove names, specifics) and use an approved enterprise AI tool. For example: "Draft an email apologizing for a project delay" (describe the situation generally without client details).

Q: Who decides if data is properly sanitized?

A: You do initially, but when working with Confidential data, your department head or designated approver reviews before you proceed. Use the sanitization guide above as your standard.

Q: What about data from third parties (vendors, partners)?

A: Treat it at the same tier as your own data of that type. A vendor's pricing proposal to you is Confidential (Tier 3) even though it is their data.

**Q: Can I take screenshots of AI conversations that include work data?**

A: Only if the data in the conversation meets the tier requirements. Screenshots should be treated with the same sensitivity as the underlying data. Store them securely.

Q: We have a U.S. office and a Canadian office. Do we need two classification systems?

A: No. Use one four-tier system for the whole company. The tiers are the same; only the legal labels and the regulators differ, and the marked boxes in this template give you both. The one place to be careful is cross-border transfer: data about Canadian individuals that moves to a U.S. tool or office is still governed by Canadian law, and Quebec adds the privacy impact assessment step.

ENFORCEMENT AND CONSEQUENCES

What happens if someone violates data classification rules?**First-time unintentional violation:**

- Coaching and retraining
- Documentation in personnel file (minor)
- Additional monitoring of AI usage

Repeated or negligent violations:

- Formal written warning
- Temporary restriction of AI tool access
- Required re-certification on policies
- Performance improvement plan

Intentional violations or gross negligence:

- Suspension or termination
- Potential legal action
- Reporting to regulatory bodies if required

BOTH COUNTRIES

Reporting to regulatory bodies means: in Canada, the Office of the Privacy Commissioner of Canada (and the Alberta Commissioner or Quebec's CAI where those laws apply) as soon as feasible when a breach creates a real risk of significant harm, plus notice to affected individuals and a breach record kept for 24 months; in the United States, the state attorney general and affected residents under the breach law of each state where they live (all 50 states have one; most set a 30- to 60-day outer limit), plus HHS within 60 days for HIPAA breaches. See the When to Escalate card for who to call.

Our goal is education and prevention, not punishment. Report concerns and mistakes immediately.

PERIODIC REVIEW SCHEDULE

This classification system should be reviewed:

- Quarterly: spot check that classifications remain appropriate
- Annually: formal review with all department heads
- As needed: when new data types emerge or regulations change (in both countries, that is often)
- After incidents: if a data leak or breach occurs

Next scheduled review: _____



Responsible party: _____

APPROVAL AND SIGN-OFF

Data Classification System approved by:

CEO: _____

CFO/COO: _____

IT/Security Lead: _____

General Counsel (if applicable): _____

Privacy Officer (required in Quebec; recommended everywhere): _____

Communication to team:

Date announced: _____

☒ All-hands ☐ Email ☐ Training ☐ Other: _____

Training completion deadline: _____



QUICK REFERENCE CARD

Print this page for easy desktop reference.

Tier	Colour	AI usage	Examples
PUBLIC	Green	Any AI tool	Website content, published materials, public research
INTERNAL	Yellow	Enterprise tools only	Meeting notes, org charts, internal training, policies
CONFIDENTIAL	Orange	Sanitize + approval	Client data, financials, contracts, pricing, competitive intel; Quebec personal data needs a PIA before transfer
RESTRICTED	Red	Executive approval only	Trade secrets, legal privilege, M&A, board materials, SSN/SIN and other government IDs, health records

Remember:

- When in doubt, classify UP (more restrictive)
- Sanitize before using AI with Confidential data
- Get approval when required
- Report mistakes immediately
- Use enterprise tools for Internal data and above
- Data about Canadian individuals stays under Canadian law even when it crosses the border, and the reverse is true for U.S. state residents

Questions? Contact: _____

Document Version: 2.0 Canadian Edition (US and Canada) | Last updated: September 2026 | Based on Version 1.0, November 2025. © Elliptic Systems Corporation | EllipticSystems.com. Educational material, not legal advice. Laws and regulator guidance change; confirm current requirements before relying on this document.



ARTIFICIAL INTELLIGENCE (AI) USAGE POLICY

[YOUR COMPANY NAME]

United States and Canada edition

Effective Date: _____

Policy Owner (Title): _____

Privacy Officer (required for Quebec operations; recommended everywhere):

Review Schedule: Quarterly Version: 2.0

1. PURPOSE AND SCOPE

1.1 Purpose. This policy establishes guidelines for the responsible use of Artificial Intelligence (AI) tools and services by [Company Name] employees, contractors, and authorized third parties. Our goal is to enable productivity and innovation through AI while protecting our company's data, intellectual property, and legal obligations in every jurisdiction where we operate.

1.2 Scope. This policy applies to:

- All AI-powered tools and services used for company business
- Both company-provided and personally-owned devices accessing company data
- All employees, contractors, consultants, and temporary workers, in the United States and in Canada
- All data classifications (Public, Internal, Confidential, Restricted)

1.3 Policy statement. [Company Name] recognizes AI as a strategic asset that enhances productivity, creativity, and decision-making. We support responsible AI usage that aligns with our values, protects stakeholder interests, and complies with legal and regulatory requirements.

BOTH COUNTRIES

1.4 Governing law. Personal information handled by our Canadian operations, or about Canadian residents, is governed by the Personal Information Protection and Electronic Documents Act (PIPEDA) and, where applicable, British Columbia's PIPA, Alberta's PIPA, Quebec's Law 25 and provincial health privacy laws. Personal information handled by our U.S. operations, or about U.S. residents, is governed by applicable federal sector laws (HIPAA, GLBA, COPPA, FERPA) and state privacy and breach-notification laws (including California's CCPA/CPRA). Where the two differ, employees follow the stricter rule.

2. APPROVED AI TOOLS

2.1 Company-approved AI tool stack. Employees may ONLY use the following AI tools for company business:

PRODUCTIVITY AI (writing, email, documents, meetings)

Primary (e.g., Microsoft 365 Copilot): _____

Alternative (e.g., Google Workspace AI): _____

Purpose: drafting communications, summarizing documents, meeting transcription. Data tier allowed: Public, Internal, Confidential (sanitized only).

CREATIVE AI (graphics, design, video, marketing)

Primary (e.g., Adobe Firefly): _____

Alternative (e.g., Canva AI): _____



Purpose: creating marketing materials, graphics, presentations. Data tier allowed: Public, Internal (non-confidential projects). All outputs must use commercially-licensed models to avoid copyright issues.

DEVELOPMENT AI (code, documentation, technical writing)

Primary (e.g., GitHub Copilot): _____

Alternative (e.g., Cursor): _____

Purpose: code generation, debugging, technical documentation. Data tier allowed: Public, Internal (code review required before deployment). All AI-generated code must undergo security review before production use.

ANALYSIS AND RESEARCH AI (data analysis, research, decision support)

Primary (e.g., Claude for Business): _____

Alternative (e.g., ChatGPT Enterprise): _____

Purpose: research, data analysis, business intelligence, strategic planning. Data tier allowed: Public, Internal, Confidential (with sanitization and approval).

Data hosting region for each approved tool (US / Canada / other): _____

2.2 Consumer AI tools. Consumer or free versions of AI tools (ChatGPT Free, Claude.ai free, Gemini, etc.) may ONLY be used with Public (Tier 1) data. Do not use personal AI accounts for any company business involving Internal, Confidential, or Restricted data.

2.3 Requesting new AI tools. Employees who identify a new AI tool that could benefit company operations should:

- Submit a request to [IT/Security Department] using the New Tool Request Form
- Include business justification and expected ROI
- Identify the data classification tiers that would be used and the countries whose data would be involved
- Allow 2-3 weeks for evaluation and security review

Do not begin using unapproved AI tools while your request is pending.

3. DATA CLASSIFICATION AND AI USAGE RULES

3.1 Four-tier classification system. [Company Name] uses a four-tier data classification system. You must understand which tier your data falls into before using AI tools. [Reference: AI Data Classification Template, US and Canada edition, for detailed examples and the decision tree.]

Tier	AI usage	Examples	Prohibited
Tier 1: PUBLIC	Unrestricted, any AI tool	Published marketing, public website content, general research	
Tier 2: INTERNAL	Company-approved enterprise AI tools only	Internal meeting notes, policies, project plans, org charts	Consumer or free AI accounts, personal subscriptions
Tier 3: CONFIDENTIAL	Restricted: sanitization + department head approval	Client data, financial details, pricing, contracts; personal information of customers and employees	Any unsanitized input; any consumer tool



Tier	AI usage	Examples	Prohibited
Tier 4: RESTRICTED	Prohibited without written executive approval	Trade secrets, privileged communications, M&A, board materials; SSN (US) and SIN (Canada), health records	Everything without CEO/CFO/General Counsel sign-off

Tier 3 requirements: remove all personally identifiable information; generalize specifics (names, numbers, dates); document AI usage and purpose; get manager or department head sign-off; use only approved enterprise AI tools.

Tier 4 requirements: CEO, CFO, General Counsel, or designated executive must approve in writing; maximum security controls applied; complete audit trail maintained; may require a specialized secure environment.

CANADA

Personal information about Quebec residents may not be entered into an AI tool hosted outside Quebec until a privacy impact assessment (PIA) has been completed and documented, as Law 25 requires. The Privacy Officer owns the PIA.

UNITED STATES

"Sensitive personal information" as defined by state privacy laws (precise geolocation, biometric identifiers, health, financial account details, immigration status, data about children under 13) is Tier 4 and needs the individual's opt-in consent before any processing, AI or otherwise.

3.2 "When in doubt" rule. If you are uncertain which tier your data falls into, classify UP (more restrictive) and ask your manager or IT/Security before proceeding.

4. ACCEPTABLE USE GUIDELINES

4.1 AI tools SHOULD be used for:

- Drafting and editing written communications (emails, reports, proposals)
- Summarizing long documents or meeting transcripts
- Research and information gathering
- Brainstorming and ideation
- Data analysis and visualization
- Creating marketing content and graphics
- Code generation and debugging (with review)
- Language translation, including English and French for Canadian operations (a human reviews anything published or sent to a customer)
- Meeting preparation and follow-up
- Learning and professional development

4.2 AI tools MUST NOT be used for:

- Processing Restricted (Tier 4) data without executive approval
- Making final decisions on hiring, termination, or promotions without human review
- Providing medical, legal, or financial advice to clients without professional review
- Creating deepfakes or manipulated media intended to deceive
- Generating content that violates copyright, trademark, or intellectual property rights
- Bypassing security controls or access restrictions



- Harassing, discriminating against, or defaming individuals
- Conducting unauthorized surveillance or monitoring of employees or customers
- Any illegal, unethical, or fraudulent activity

BOTH COUNTRIES

Automated decisions about people. Quebec's Law 25 requires that individuals be told when a decision about them was made solely by automated processing, and be given a way to have it reviewed by a person. Several U.S. states (Colorado, California) and New York City impose similar notice, opt-out or bias-audit duties for AI used in hiring and other significant decisions. Our rule in both countries: a human makes the final call, and we can explain it.

4.3 Human oversight required. AI is a tool to augment human decision-making, not replace it. Employees must review and verify AI-generated content for accuracy, apply professional judgment before acting on AI recommendations, take responsibility for work product even if AI-assisted, and disclose AI usage when required (see Section 5).

5. DISCLOSURE AND TRANSPARENCY

5.1 Internal disclosure. When AI generates significant work product, employees should document AI usage in project files or communications. "Significant work product" includes client deliverables or proposals, strategic plans or recommendations, financial analyses or projections, legal documents or contracts, and code deployed to production. Example disclosure: "This analysis was developed with AI assistance and has been reviewed and verified by [Your Name]."

5.2 External disclosure. When providing AI-generated content to external parties (clients, partners, regulators): disclose AI usage if the recipient has a reasonable expectation of human-only work; ensure all content is reviewed by qualified professionals; never misrepresent AI-generated content as entirely human-created when disclosure is expected.

5.3 Client-specific requirements. Some clients may prohibit or restrict AI usage. Always check client contracts and communications for AI restrictions before using AI on client matters. Government and public-sector clients in both countries commonly impose such restrictions, and several Canadian public bodies (federal, BC, Nova Scotia) restrict where their data may be stored.

6. DATA SECURITY AND PRIVACY

6.1 Data sanitization requirements. Before inputting Confidential (Tier 3) data into AI tools, employees must sanitize by: removing or replacing names with generic identifiers ("Client A," "Employee 1"); redacting or rounding financial figures to ranges; generalizing dates, locations, and identifying details; removing contact information (emails, phone numbers, addresses). [Reference: AI Data Classification Template, "Data Sanitization Guide."]

6.2 Prohibited data sharing. NEVER input the following into AI tools without explicit executive approval:

- Government identifiers: Social Security numbers (US); Social Insurance Numbers and health card numbers (Canada); driver's licence and passport numbers (both)
- Financial account numbers and credit card information
- Passwords, access tokens, API keys, or credentials
- Attorney-client or solicitor-client privileged communications
- Protected health information (HIPAA PHI in the US; personal health information under provincial law in Canada)
- Personal information of minors
- Trade secrets or proprietary algorithms



6.3 Privacy law compliance. [Company Name] handles personal information in accordance with the laws named in Section 1.4. In practice this means: we collect and use personal information only for purposes the individual would reasonably expect and has been told about; we do not enter personal information into an AI tool that is not on the approved list with a data processing agreement in place; we honour access, correction and deletion requests from individuals in both countries; and the Privacy Officer is the point of contact for any privacy question.

CANADA

PIPEDA does not forbid storing Canadian personal information outside Canada, but it requires that the information receives comparable protection wherever it goes and that individuals are told it may be processed abroad. Our privacy notice says so. Quebec adds the PIA requirement in Section 3.1.

UNITED STATES

There is no general U.S. restriction on where data is stored. Sector rules apply instead: HIPAA business associate agreements for health data, GLBA safeguards for financial data, and contractual data-location clauses from government and defence customers.

6.4 Data retention and deletion. Be mindful that AI conversations may be retained by vendors. Delete sensitive AI conversations when no longer needed. Do not use AI chat history as permanent record storage. Use company-approved document management systems for official records.

7. INTELLECTUAL PROPERTY AND COPYRIGHT

7.1 IP ownership. [Company Name] owns all work product created by employees, including AI-assisted content. Employees should not input company IP into AI tools that use data for model training (check vendor terms). Ensure enterprise AI tools have opted out of training data usage.

7.2 Copyright compliance. Use only commercially-licensed AI tools for creating external-facing content. Do not use AI to generate content that infringes on others' copyrights or trademarks. Verify that AI-generated images, text, or code are free from copyright concerns before publication. When in doubt, consult Legal before publishing AI-generated content externally.

BOTH COUNTRIES

Neither the U.S. Copyright Office nor Canadian courts currently recognize copyright in work generated by AI without meaningful human authorship. Treat purely AI-generated output as unprotectable and keep records of the human contribution to anything we intend to own.

7.3 Third-party content. Do not upload copyrighted materials (books, articles, proprietary documents) to AI tools without proper authorization. Respect the licensing terms of any third-party content processed through AI.

8. BIAS, FAIRNESS AND ETHICAL CONSIDERATIONS

8.1 Awareness of AI limitations. Employees must understand that AI tools can generate plausible-sounding but inaccurate information ("hallucinations"), may reflect biases present in training data, cannot replicate human judgment, empathy, or ethical reasoning, and should not be the sole basis for important decisions.

8.2 Bias mitigation. When using AI for decisions affecting people (hiring, performance reviews, customer service): use AI as one input among many, not the sole decision-maker; review AI recommendations for potential bias or discrimination; ensure diverse human oversight of AI-assisted decisions; document the decision-making process including AI's role. Human rights and anti-discrimination law applies to AI-assisted decisions in both countries (the Canadian Human



Rights Act and provincial codes; Title VII, the ADA and state law in the U.S.).

8.3 Ethical use. Employees should consider: Could this AI usage harm individuals or groups? Am I being transparent about AI's role? Would I be comfortable if this AI usage were made public? Does this align with our company values?

9. VENDOR MANAGEMENT AND CONTRACTS

9.1 Approved vendors only. Use only AI vendors that have been vetted by [Company Name] and meet our security and privacy requirements.

9.2 Required vendor commitments. Our approved AI vendors must provide:

- Data Processing Agreements (DPAs) protecting our data
- Opt-out from using our data for model training, in writing
- SOC 2 Type II or ISO 27001 certification, or an equivalent (CyberSecure Canada is acceptable evidence for smaller Canadian vendors)
- Clear data residency and sovereignty terms, including where our data is stored and processed and whether a Canadian region is available
- Breach notification to us fast enough for us to meet our own legal deadlines (24 hours preferred; 72 hours maximum)
- Data portability and deletion guarantees
- Confirmation that they meet the sector rules that apply to us (HIPAA business associate agreement, PCI DSS, provincial health privacy law)

9.3 Personal AI subscriptions. Employees who maintain personal subscriptions to AI tools (e.g., ChatGPT Plus) should use separate accounts for personal and company business, never mix company data into personal AI accounts, and understand that personal AI accounts are not approved for company business.

10. TRAINING AND COMPETENCY

10.1 Required training. All employees must complete AI Usage Policy training within 30 days of hire or policy implementation, annual refresher training, and additional training when significant policy updates occur.

10.2 Role-specific training. Managers and department heads: approving Confidential data AI usage, monitoring team compliance. IT/Security: AI tool evaluation, security controls, incident response. Legal/Compliance and the Privacy Officer: AI in regulated activities, contract reviews, disclosure requirements, cross-border transfer rules. Developers: secure coding with AI, code review practices.

10.3 Staying current. AI technology and the law around it evolve rapidly. Employees should stay informed about updates to company AI tools and policies, report new AI use cases or tools to IT for evaluation, and share AI best practices and lessons learned with colleagues.

11. MONITORING AND ENFORCEMENT

11.1 Monitoring. [Company Name] reserves the right to monitor AI tool usage and data accessed, review AI conversation logs and outputs, audit compliance with this policy, and block access to unapproved AI tools. Monitoring protects both the company and employees by ensuring appropriate AI usage.



CANADA

Employee monitoring in Canada must be reasonable and disclosed. Ontario requires a written electronic monitoring policy for employers with 25 or more employees, and privacy commissioners in BC, Alberta and Quebec expect monitoring to be proportionate to a real business need. This section, once signed, is our disclosure.

UNITED STATES

Most U.S. states permit monitoring of company systems with notice; Connecticut, Delaware and New York require written notice to employees. This section, once acknowledged in Section 17, is our notice.

11.2 Reporting concerns. Employees should report suspected policy violations, AI-related security incidents or data leaks, concerns about AI bias or ethical issues, and suggestions for policy improvements. Report to: [IT/Security Department email/phone] or [Manager/HR]. Non-retaliation: employees will not be penalized for good-faith reporting of concerns.

11.3 Consequences of violations. First-time unintentional violations: coaching and additional training, documentation in personnel file, temporary enhanced monitoring. Repeated or negligent violations: formal written warning, restriction of AI tool access, performance improvement plan, potential disciplinary action up to termination. Intentional violations or gross negligence: suspension or termination of employment, legal action if warranted, reporting to authorities if legally required. Our goal is education and compliance, not punishment. Report mistakes immediately to minimize harm.

12. ROLES AND RESPONSIBILITIES

12.1 Employees: understand and comply with this policy; complete required training; classify data appropriately before AI usage; report concerns and incidents promptly; use AI as a tool to enhance, not replace, professional judgment.

12.2 Managers and department heads: ensure team members understand and follow the policy; approve Confidential data AI usage when requested; monitor for compliance in their department; support employees in responsible AI adoption.

12.3 IT/Security: maintain the approved AI tool stack; evaluate new AI tool requests; implement technical controls and monitoring; respond to AI-related security incidents; provide technical guidance and support.

12.4 Legal/Compliance: review AI vendor contracts; advise on regulatory compliance in each country; handle legal aspects of AI-related incidents; update the policy for legal and regulatory changes.

12.5 Privacy Officer: accountable for personal information handling under PIPEDA and provincial law (a named privacy officer is mandatory under Quebec Law 25 and defaults to the CEO if no one is appointed); completes privacy impact assessments; owns breach assessment and regulator reporting in both countries; answers individual access and deletion requests.

12.6 Executive leadership: approve Restricted data AI usage requests; allocate resources for AI tools and training; set strategic direction for AI adoption; review policy effectiveness quarterly.

13. INCIDENT RESPONSE

13.1 What constitutes an AI incident? Confidential or Restricted data uploaded to an unapproved AI tool; suspected data leak through an AI tool; AI-generated content causing harm or reputational damage; discovery of bias or discrimination in AI-assisted decisions; breach of client-specific AI restrictions.



13.2 If you suspect an incident:

STEP 1: STOP. Stop using the AI tool immediately. Do not delete conversations or evidence.

STEP 2: REPORT. Notify [IT/Security] immediately: [Contact Info]. Contact your manager. Document what happened.

STEP 3: COOPERATE. Provide information for the investigation. Follow remediation instructions. Complete any additional required training.

Remember: quick reporting minimizes damage. You will not be punished for honest mistakes reported promptly.

13.3 Legal reporting duties (Incident Lead and Privacy Officer). Where an incident involves personal information, the Incident Lead and Privacy Officer assess within the first day whether it creates a real risk of significant harm to individuals, and then:

CANADA

Report to the Office of the Privacy Commissioner of Canada as soon as feasible (and to the Alberta Commissioner or Quebec's CAI where those laws apply); notify affected individuals directly and any organization that can reduce the harm; record every breach, reported or not, and keep the record for at least 24 months. Knowingly failing to report or record is an offence under PIPEDA with fines up to CA\$100,000 per violation; Quebec penalties run up to the greater of CA\$25 million or 4% of worldwide turnover. Report cyber incidents to the Canadian Centre for Cyber Security (cyber.gc.ca) and fraud to the Canadian Anti-Fraud Centre (1-888-495-8501).

UNITED STATES

Notify affected residents and, in most states, the state attorney general under the breach-notification law of every state where affected individuals live; most set a 30- to 60-day outer limit and several require notice "without unreasonable delay." HIPAA breaches: notify HHS (within 60 days, or annually for breaches under 500 people) and, for breaches over 500, the media. Report cyber incidents to CISA (cisa.gov/report) and the FBI's IC3 (ic3.gov). Publicly traded companies: assess SEC Form 8-K materiality within four business days.

14. EXCEPTIONS AND WAIVERS

14.1 Requesting an exception. In rare cases an exception may be necessary. Employees should submit a written request to [Policy Owner] explaining what policy provision needs an exception, the business justification, alternative controls to mitigate risk, and the duration needed; obtain approval from the appropriate authority; and document the exception and review it regularly.

14.2 Approval authority. Public/Internal data exceptions: Department Head. Confidential data exceptions: VP or C-suite. Restricted data exceptions: CEO, CFO, or General Counsel. Any exception involving cross-border transfer of personal information: Privacy Officer must also sign.

15. POLICY REVIEW AND UPDATES

15.1 Review schedule. Quarterly by IT/Security and the Policy Owner; annually by executive leadership; as needed when significant AI developments, incidents, or regulatory changes occur in either country.

15.2 Updates and communication. Policy updates will be communicated via [email/intranet/all-hands meeting]. Employees will be notified of material changes and may need to re-certify. Version history will be maintained.

Next scheduled review: _____



16. RELATED POLICIES AND RESOURCES

This policy works in conjunction with the Data Classification Policy, Information Security Policy, Acceptable Use Policy, Bring Your Own Device (BYOD) Policy, Social Media Policy, Electronic Monitoring Policy (Ontario), and Code of Conduct. Additional resources: AI Data Classification Template; Vendor Evaluation Scorecard; Daily Defense Checklist (Leadership Edition); 5 Critical Decisions Worksheet; When to Escalate card.

17. ACKNOWLEDGMENT AND CERTIFICATION

I acknowledge that I have read, understood, and agree to comply with [Company Name]'s Artificial Intelligence Usage Policy. I understand that violations may result in disciplinary action up to and including termination; that I am responsible for understanding data classification before using AI; that I must report incidents and concerns promptly; that company systems may be monitored as described in Section 11; and that this policy may be updated and I will be notified of changes.

Employee name (print): _____

Employee signature: _____

Date: _____

Manager name (print): _____

Manager signature: _____

Date: _____

18. POLICY APPROVAL

CEO: _____

CFO/COO: _____

CIO/CISO: _____

General Counsel: _____

Privacy Officer: _____



APPENDIX A: QUICK REFERENCE GUIDE

Data classification quick check

If your data is...	Then you can use...
Public (marketing, website, published info)	Any AI tool
Internal (meeting notes, policies, schedules)	Enterprise tools only
Confidential (client data, financials, pricing, personal information)	Sanitize + get approval + enterprise tools; Quebec personal data needs a PIA before it leaves Quebec
Restricted (trade secrets, legal privilege, M&A, government IDs, health records)	Executive approval required

Key reminders

- When in doubt, classify UP and ask before proceeding
- Sanitize Confidential data before AI input
- Use enterprise tools for anything beyond Public data
- Report incidents immediately; no punishment for honest mistakes
- Review AI outputs; do not trust blindly
- A human makes the final decision about a person, in both countries

APPENDIX B: FREQUENTLY ASKED QUESTIONS

Q: Can I use ChatGPT for work? A: Only the ChatGPT Enterprise version (if approved) for Internal data and above. ChatGPT Free/Plus is fine for Public data only.

Q: I found a great new AI tool. Can I use it? A: Submit a New Tool Request. Do not use it while waiting for approval if you will be working with company data.

Q: What if a client says "don't use AI on our project"? A: Honour that restriction completely. Client requirements override this policy.

Q: Can I use AI to write emails to clients? A: Yes, as long as you sanitize any confidential client information and review before sending.

Q: What if AI gives me wrong information? A: Always verify AI outputs. You are responsible for accuracy, not the AI.

Q: I accidentally uploaded confidential data to ChatGPT. What do I do? A: Report immediately to IT/Security and your manager. Do not delete the conversation yet.

Q: Our customer is in Quebec and our AI tool is hosted in Virginia. Is that allowed? A: Only after the Privacy Officer has completed and documented a privacy impact assessment for the transfer, and only if the tool is on the approved list with a DPA. Ask before you upload.

Q: We had a breach affecting customers in both Ontario and California. Who do we tell? A: Both. The Privacy Officer reports to the Office of the Privacy Commissioner of Canada and notifies the Ontario customers; Legal notifies the California customers and the California Attorney General under California's breach law. Each country's clock runs separately. See Section 13.3 and



the When to Escalate card.

APPENDIX C: REGULATOR AND AGENCY CONTACTS

Purpose	Canada	United States
Privacy regulator	Office of the Privacy Commissioner of Canada, priv.gc.ca , 1-800-282-1376; provincial: BC OIPC, Alberta OIPC, Quebec CAI	State attorneys general (breach notice); FTC (unfair or deceptive practices); HHS Office for Civil Rights (HIPAA)
Cyber incident reporting	Canadian Centre for Cyber Security, cyber.gc.ca	CISA, cisa.gov/report ; FBI Internet Crime Complaint Center, ic3.gov
Fraud and phishing	Canadian Anti-Fraud Centre, 1-888-495-8501	FTC, reportfraud.ftc.gov ; FBI IC3
Small-business security baseline	Canadian Centre for Cyber Security Baseline Controls; CyberSecure Canada certification	NIST Cybersecurity Framework 2.0; CISA Cyber Essentials

Document Version: 2.0 (US and Canada) Effective Date: _____

Next Review Date: _____

© [Company Name] | [Year]. Policy template provided by Elliptic Systems Corporation; Canadian edition prepared September 2026. Educational material, not legal advice. Laws and regulator guidance in both countries change frequently; confirm current requirements with your legal advisor before relying on this document.



THE 5 CRITICAL INFRASTRUCTURE DECISIONS

Building Your Secure AI-Enabled Workplace

United States and Canada edition

Company name: _____

Decision date: _____

Leadership team: _____

Countries where we have offices, employees or customers: _____

PURPOSE

This worksheet forces you to make, and document, the five critical decisions that enable safe AI adoption in your organization. Complete it within 30 days of Session 4. If you operate on both sides of the border, make each decision once for the whole company and use the marked boxes to record where the U.S. and Canadian rules differ.

DECISION #1: DATA CLASSIFICATION FOR AI USE

The question: What data can we safely use with AI tools, and what must be restricted?

Your four-tier classification

TIER 1: PUBLIC. Safe for any AI tool (consumer or enterprise)

Examples for your business:

1. _____
2. _____
3. _____

Who decides if data is Public? _____

TIER 2: INTERNAL. Company information requiring approved enterprise AI tools only

Examples for your business:

1. _____
2. _____
3. _____

Approved AI tools for Internal data:

1. _____
2. _____

TIER 3: CONFIDENTIAL. Client data, financials: restricted AI use with specific controls

Examples for your business:

1. _____
2. _____
3. _____

Required controls for Confidential data:

- Data must be sanitized/anonymized before AI input



- Only approved enterprise tools with a DPA (Data Processing Agreement)
- Department head approval required
- Activity logging and audit trail
- Privacy impact assessment before personal information about Quebec residents leaves Quebec
- Other: _____

TIER 4: RESTRICTED. Trade secrets, M&A, privileged legal: no AI without executive approval

Examples for your business:

1. _____
2. _____
3. _____

BOTH COUNTRIES

Add to your Tier 4 list, whichever country the data comes from: Social Security numbers (US), Social Insurance Numbers and health card numbers (Canada), driver's licence and passport numbers, health records, and "sensitive personal information" as defined by U.S. state privacy laws.

Who can approve Restricted data AI use?

- CEO only
- CEO + CFO + Legal
- Executive Committee vote
- Other: _____

Named Privacy Officer (mandatory for Quebec operations under Law 25; PIPEDA requires an accountable person everywhere in Canada): _____

Decision documentation

We have defined our four data classification tiers: YES / NO

Classification guide has been documented and shared: YES / NO

Employees can easily determine which tier their data falls into: YES / NO

Consequences for misclassification are clear: YES / NO

DECISION #2: APPROVED AI TOOL STACK

The question: Which AI tools will we officially support, and for what purposes?

PRODUCTIVITY AI (writing, email, document creation, meeting summaries)

Primary: _____

Alternative: _____

License type: [] Enterprise [] Business [] Consumer

Data Protection Agreement in place? YES / NO

Data hosting region (US / Canada / other): _____

Teams/roles who can use: _____

CREATIVE AI (graphics, design, video, marketing content)

Primary: _____



Alternative: _____

Commercial licensing confirmed? YES / NO

Copyright/IP ownership clarified? YES / NO

Teams/roles who can use: _____

DEVELOPMENT AI (code generation, debugging, documentation)

Primary: _____

Alternative: _____

Code review process required? YES / NO

Security scanning integrated? YES / NO

Teams/roles who can use: _____

ANALYSIS AI (data analysis, research, decision support)

Primary: _____

Alternative: _____

Data residency requirements met? YES / NO

Audit logging enabled? YES / NO

Teams/roles who can use: _____

Tool procurement process

Who approves new AI tool requests?

- ☐ IT/Security Lead
- ☐ Department Head + IT
- ☐ Executive Committee
- ☐ Other: _____

Evaluation criteria (rank 1-5 in importance):

Security/compliance certifications _____

Integration with existing tools _____

User-friendliness and adoption potential _____

Cost and ROI _____

Vendor reputation and support _____

Request process: _____

Decision documentation

We have documented our approved AI tool stack: YES / NO

Tool stack has been communicated to all employees: YES / NO

Process exists for requesting new tools: YES / NO

Unsupported tools are blocked or monitored: YES / NO

DECISION #3: AI USAGE POLICIES

The question: What are the clear rules for how employees use AI tools?

When AI is encouraged. AI should be used for:

1. _____
2. _____



3. _____

4. _____

When AI is prohibited. AI must NOT be used for:

1. _____

2. _____

3. _____

4. _____

BOTH COUNTRIES

Whatever else is on your prohibited list, include "making a final decision about a person (hiring, firing, credit, pricing, service) without human review." Quebec's Law 25, Colorado's AI Act, New York City's hiring-tool law and California regulations all impose notice, review or audit duties on automated decisions about people.

Data sanitization requirements. Before inputting data into AI, employees must:

- Remove client/customer names
- Redact specific financial figures
- Generalize identifying details
- Remove email addresses and phone numbers
- Other: _____

Training provided on how to sanitize data? YES / NO

Exception approval process. If an employee needs to do something outside standard policy:

Step 1: _____

Step 2: _____

Who can grant exceptions? _____

Documentation required: ☐ Email ☐ Form ☐ Meeting ☐ Other: _____

AI output requirements. When AI generates significant work product, employees must:

- Disclose that AI was used
- Review and verify accuracy
- Document in project files
- Get manager approval before external use
- Other: _____

"Significant work product" is defined as: _____

Decision documentation

We have written AI usage policies in plain English (and French, where we have Quebec employees): YES / NO

Policies have been shared with the entire team: YES / NO

Employees can easily find and reference policies: YES / NO

Enforcement process is clear and consistent: YES / NO

DECISION #4: ACCESS ARCHITECTURE FOR REMOTE AI WORK

The question: How do we secure AI usage when employees work from anywhere, including across the border?

Cloud security approach. Our security model is:



- Cloud-first (security follows users anywhere)
- Hybrid (some on-premise, some cloud)
- Primarily on-premise with VPN for remote

Cloud security tools we are using: _____

Browser vs. desktop applications. Our policy on AI tool access methods:

- Browser-based tools only (easier to monitor/control)
- Desktop applications allowed (better performance)
- Case-by-case basis depending on tool
- Other: _____

Browser security extensions required: _____

Network segmentation. AI development/experimental environments are:

- Completely separated from production systems
- Partially segmented with controlled access
- Not currently segmented (plan to implement)
- Not applicable (we do not develop AI internally)

If segmented, what can AI environments access: _____

BYOD (Bring Your Own Device) policy. Personal devices accessing company AI tools:

- Allowed with Mobile Device Management (MDM)
- Allowed for approved apps only
- Allowed with security requirements (list below)
- Not allowed (company devices only)

If allowed, required security measures:

- Encrypted storage
- PIN/biometric lock
- Remote wipe capability
- Updated OS and security patches
- Approved AI apps only (no sideloading)
- Other: _____

Home network security. Requirements for employees working from home:

- Updated router firmware
- Changed default router password
- Separate guest Wi-Fi for family/visitors
- VPN required for accessing company systems
- Other: _____

Support provided for home network security:

- How-to guides
- IT help desk support
- One-time stipend for equipment
- Other: _____

Data residency for remote and cross-border work



CANADA

PIPEDA allows Canadian personal information to be stored or accessed outside Canada if it gets comparable protection and individuals are told. Public bodies in BC and Nova Scotia, and many Canadian government contracts, restrict where their data may sit; if you serve them, record the restriction here. Quebec personal information leaving Quebec needs a documented privacy impact assessment first.

UNITED STATES

There is no general U.S. data-location rule for private companies. Federal, defence (CMMC, ITAR) and some state-government customers require U.S.-only storage and U.S.-person access; if you hold such contracts, Canadian staff may need to be walled off from that data. Record the restriction here.

Our data residency rule for remote and cross-border access: _____

Decision documentation

We have defined our remote access architecture: YES / NO

BYOD policy is documented and communicated: YES / NO

Employees understand home network requirements: YES / NO

Technical support is available for remote setup: YES / NO

Cross-border data access rules are written down: YES / NO

DECISION #5: AI VENDOR RISK MANAGEMENT

The question: What vendor commitments are non-negotiable before we adopt AI tools?

Data residency requirements. Our data must be stored:

- ☐ In United States data centres only
- ☐ In Canadian data centres only
- ☐ In the U.S. or Canada, with the location disclosed in writing
- ☐ In specific regions (list): _____
- ☐ No restriction (any vendor location acceptable)

Vendor must provide written confirmation: YES / NO

Training data opt-out. Our data being used to train or improve AI models:

- ☐ Absolutely prohibited (must opt out in contract)
- ☐ Acceptable for aggregate/anonymized data only
- ☐ Acceptable with disclosure
- ☐ No restriction

Vendor must provide an opt-out mechanism: YES / NO

Required security certifications. Vendors must have (check all required):

- ☐ SOC 2 Type II (within last 12 months)
- ☐ ISO 27001
- ☐ CyberSecure Canada certification (a strong signal for a smaller Canadian vendor)
- ☐ HIPAA compliance and a business associate agreement (US health data)
- ☐ Provincial health privacy compliance: PHIPA, PIPA, HIA (Canadian health data)
- ☐ PCI DSS (payment data, both countries)
- ☐ CMMC Level ____ (US defence contractors)



- Bill C-8 / Critical Cyber Systems Protection Act awareness (Canadian finance, telecom, energy, transportation, and their suppliers)
- Other: _____

We will verify certifications before contract signature: YES / NO

Contract requirements. Our AI vendor contracts must include:

- Clear data ownership terms (we own our data)
- Data portability (we can export our data)
- Right to audit vendor security practices
- Breach notification within 24 / 48 / 72 hours (circle one)
- Liability caps and insurance requirements
- Service Level Agreements (SLAs) with penalties
- Termination terms and data deletion guarantee
- Price lock or maximum annual increase
- Governing law and venue we can afford to litigate in (a Canadian company signing a U.S.-only contract, or the reverse, should think twice)
- Other: _____

BOTH COUNTRIES

Why the notification clock matters. Canada: PIPEDA requires you to report a breach to the Privacy Commissioner "as soon as feasible." United States: state laws set 30- to 60-day outer limits and HIPAA sets 60 days, but several states and the SEC (four business days for material incidents at public companies) run faster. You cannot meet any of these if your vendor takes a week to tell you. Ask for 24 hours; do not accept more than 72.

Vendor evaluation process. Before selecting an AI vendor, we will:

- Complete the Vendor Evaluation Scorecard
- Check 3+ customer references
- Review security documentation
- Conduct a pilot/trial period
- Have legal review contract terms (in the country whose law governs)
- Get executive sign-off

Minimum scorecard score to proceed (out of 5.0): _____

Business continuity planning. If our primary AI vendor fails or changes terms unacceptably:

Backup vendor option 1: _____

Backup vendor option 2: _____

Data export and migration plan: _____

Maximum acceptable downtime (hours/days): _____

Decision documentation

We have defined non-negotiable vendor requirements: YES / NO

Legal team has reviewed contract requirements: YES / NO

Vendor evaluation process is documented: YES / NO

Business continuity plan exists for AI tools: YES / NO

IMPLEMENTATION TRACKING

Decision status summary



Decision	Status	Owner	Due date	Complete?
1. Data Classification				[]
2. Approved AI Tools				[]
3. Usage Policies				[]
4. Access Architecture				[]
5. Vendor Risk Management				[]

Status codes: Draft / In Review / Approved / Implemented

Communication plan. How will we communicate these decisions to the team?

- All-hands meeting
- Department-by-department training
- Email announcement with FAQ
- Updated employee handbook
- Intranet/wiki documentation
- Other: _____

Communication date: _____

Follow-up reinforcement planned: _____

30-day review

Date: _____

What is working well: _____

What needs adjustment: _____

Action item 1: _____

Action item 2: _____

Action item 3: _____

Where to look for a baseline. Canada: the Canadian Centre for Cyber Security publishes Baseline Cyber Security Controls for Small and Medium Organizations, the standard CyberSecure Canada certifies against. United States: the NIST Cybersecurity Framework 2.0 and CISA's Cyber Essentials. All are free and short. Use whichever fits your larger office, and note any gaps for the other.

Document Version: 2.0 (US and Canada) Completed: _____

Next review date: _____

© Elliptic Systems Corporation | EllipticSystems.com | Securing Your AI-Enabled Workplace. Canadian edition prepared September 2026. Educational material, not legal advice; laws in both countries change and this worksheet will need updating.



SECURITY VENDOR EVALUATION SCORECARD

Elliptic Systems Corporation | Building Secure Digital Workplaces

United States and Canada edition. The working spreadsheet with the weighting formulas is a separate download.

VENDOR INFORMATION

Vendor name: _____

Solution type: _____

Evaluated by: _____

Date: _____

Where the vendor stores and processes our data (country/region): _____

Scoring guide: rate each criterion 1-5.

Score	Meaning
1	Poor/Unacceptable. Major concerns, likely disqualifying
2	Below average. Significant gaps or weaknesses
3	Acceptable. Meets minimum requirements
4	Good. Exceeds expectations in most areas
5	Excellent. Best-in-class, exceptional capability

1. USER ADOPTION POTENTIAL (Weight: 25%)

Will your team actually use this solution, or will they find workarounds?

Factor	Score (1-5)	Notes
Intuitive interface (ease of learning)		
Integration with daily workflows		
Mobile accessibility		
User training/documentation quality (English and French if you have Quebec staff)		
Average score		

2. INTEGRATION AND COMPATIBILITY (Weight: 20%)

Does this work seamlessly with your existing technology stack?

Factor	Score (1-5)	Notes
Works with Microsoft 365/Google Workspace		
API availability for custom integrations		
Single Sign-On (SSO) support		
Compatibility with current security tools		
Average score		



3. VENDOR SUPPORT AND RELIABILITY (Weight: 20%)

Will they be there when something breaks at 2 a.m., in your time zone?

Factor	Score (1-5)	Notes
Support availability (24/7 vs. business hours; covers Pacific through Atlantic time)		
Average response time for critical issues		
Implementation/onboarding support quality		
System uptime/reliability track record		
Average score		

4. TOTAL COST OF OWNERSHIP (Weight: 15%)

What is the real cost including hidden fees, implementation, ongoing maintenance and currency?

Cost breakdown (state the currency; a USD price is roughly 35-40% more in CAD at 2026 rates, and many vendors bill Canadian customers in USD)

Licence fees (annual): _____

Implementation/setup: _____

Training costs: _____

Annual support/maintenance: _____

TOTAL YEAR 1: _____

TOTAL YEAR 2+: _____

Factor	Score (1-5)	Notes
Transparent, predictable pricing		
Implementation costs clearly stated		
No surprise fees (per-user, overage, currency conversion, etc.)		
ROI potential vs. cost		
Average score		

5. SECURITY AND COMPLIANCE (Weight: 20%)

Does this vendor protect your data and meet the regulatory requirements of every country you operate in?

Required certifications and commitments (check those that apply to your business)

Requirement	Applies when	Have it?
SOC 2 Type II (within last 12 months) or ISO 27001	Always	[]
CyberSecure Canada certification	Smaller Canadian vendors; a good sign that a small firm has a real baseline	[]



Requirement	Applies when	Have it?
PIPEDA and provincial privacy compliance (BC and Alberta PIPA, Quebec Law 25), stated in writing	Any Canadian personal information	[]
HIPAA compliance plus a signed business associate agreement	U.S. health data	[]
Provincial health privacy compliance (PHIPA, PIPA, HIA)	Canadian health data	[]
PCI DSS	Payment card data, both countries	[]
CMMC Level ____	U.S. defence contractors and their suppliers	[]
GDPR compliance	EU personal data	[]
Bill C-8 (Critical Cyber Systems Protection Act) readiness	Canadian finance, telecom, energy, transportation, and suppliers to them	[]
No training of AI models on our data, in writing	Any AI vendor	[]
Other: _____		[]

Security evaluation scoring

Factor	Score (1-5)	Notes
Security certifications (SOC 2, ISO 27001, CyberSecure Canada)		
Data residency/sovereignty controls		
Compliance with privacy and industry regulations in each country we operate in		
Incident response track record and breach-notification commitment		
Average score		

How to score the residency and notification factors

CANADA

Data residency. Score 5 if the vendor offers a Canadian region and states it in the contract; 3 if data sits in the U.S. with a signed data processing agreement and you disclose that to customers (PIPEDA allows this); 1 if the vendor cannot tell you where your data is. If you serve BC or Nova Scotia public bodies, or hold Canadian government contracts, anything below 5 may disqualify.

UNITED STATES

Data residency. There is no general U.S. residency rule for private companies. Score on contract obligations instead: federal, defence (CMMC, ITAR) and some state-government customers require U.S.-only storage and U.S.-person access. If you hold those contracts, a vendor without a U.S.-only option scores 1.

BOTH COUNTRIES

Breach notification. Score 5 for a 24-hour commitment, 3 for 72 hours, 1 for "without undue delay" with no number. In Canada you must report to the Privacy Commissioner as soon as feasible; in the U.S. state laws run 30-60 days, HIPAA 60 days, and the SEC four business days for public companies. A vendor that takes a week to tell you puts you in breach of all of them.



FINAL SCORING SUMMARY

Category	Average score	Weight	Weighted score
User adoption		25%	
Integration		20%	
Support		20%	
Total cost of ownership		15%	
Security and compliance		20%	
TOTAL WEIGHTED SCORE		100%	___ / 5.0

Decision guide: 4.0 and above, proceed; 3.0 to 3.9, proceed with conditions written into the contract; below 3.0, do not proceed. Any single security factor scored 1 is disqualifying regardless of total.

Two questions the scorecard does not ask that every owner should

- Does the contract name a governing law and a place for service that we can afford to litigate in? A Canadian company signing a U.S.-only contract (or the reverse) should price in the cost of a cross-border dispute.
- Does the vendor carry cyber insurance, and will they confirm the coverage limit in writing? It tells you whether they can make you whole if they are the cause of your breach.

Recommendation: _____

Approved by: _____

Date: _____

© Elliptic Systems Corporation | EllipticSystems.com. Canadian edition prepared September 2026. Educational material, not legal advice; requirements in both countries change and this scorecard will need updating.



DAILY DEFENSE CHECKLIST

Leadership Edition

By Elliptic Systems Corporation

Securing Your AI-Enabled Workplace, United States and Canada

YOUR 8 STRATEGIC SECURITY QUESTIONS

(Review weekly. Twenty minutes keeps you protected.)

1. AI ENABLEMENT CHECK

Question: Are we enabling AI productivity safely this week?

What to review:

- New AI tools requested by teams
- AI usage trending up or down
- Any concerns raised about AI data handling
- Any new tool that would move Canadian personal information to a U.S. host, or U.S. customer data to a Canadian host, before the privacy check was done

Red flag: team avoiding approved tools or using shadow AI.

2. POLICY COMPLIANCE

Question: Are employees following our AI/security guidelines?

What to review:

- Spot check: ask 2-3 employees what the policy is
- Review any policy exception requests
- Check for workarounds or shortcuts

Red flag: widespread confusion about what is allowed.

3. VENDOR ACCOUNTABILITY

Question: Are our vendors meeting their commitments?

What to review:

- Any service outages or performance issues
- Support response times vs. SLA
- Contract renewal dates approaching
- Any vendor notice of a security incident (their clock to tell you and your clock to tell regulators are both running)

Red flag: vendor support degrading or prices increasing unexpectedly.

4. INCIDENT AWARENESS

Question: Any security concerns raised this week?

What to review:

- Employee reports of suspicious emails or activity
- Failed login attempts or access-denied logs
- IT team escalations

Red flag: concerns being dismissed or not investigated.



BOTH COUNTRIES

Keep these on hand. Canada: Canadian Centre for Cyber Security (cyber.gc.ca) for incidents; Canadian Anti-Fraud Centre (1-888-495-8501) for phishing, invoice fraud and CEO impersonation. United States: CISA (cisa.gov/report) for incidents; FBI IC3 (ic3.gov) and FTC (reportfraud.ftc.gov) for fraud. If personal information is involved, the When to Escalate card lists the privacy regulators.

5. ACCESS AUDIT

Question: Who gained or lost system access this week?

What to review:

- New employee accounts created
- Departing employee access removed
- Role changes requiring permission updates
- Cross-border access: does anyone in the Canadian office have access to data a U.S. contract says must stay with U.S. persons, or the reverse?

Red flag: former employee still has access 48 hours after departure.

6. TRAINING STATUS

Question: Is security awareness keeping pace with change?

What to review:

- When was the last security training?
- New tools that need training
- Phishing simulation results trending
- Quebec staff: is training available in French?

Red flag: training more than 90 days old or low participation.

7. COMPLIANCE CHECKPOINT

Question: Are we meeting the regulatory requirements of every country we operate in?

What to review:

- Industry-specific compliance (both countries: PCI DSS; US: HIPAA, GLBA, CMMC; Canada: provincial health privacy law, Bill C-8 for finance, telecom, energy, transportation)
- Audit or assessment deadlines approaching
- Any compliance gaps identified

CANADA

Do we have a named privacy lead (mandatory in Quebec), a breach record kept for 24 months, and a way to report to the Office of the Privacy Commissioner as soon as feasible? Quebec: privacy impact assessment done before personal data leaves the province, consent language current. CyberSecure Canada: working toward, or maintaining, certification?

UNITED STATES

Do we know which state privacy laws apply to our customers (California, Colorado, Connecticut, Texas, Virginia and a growing list), and have we posted the required privacy notice and opt-out links? Do we know each state's breach-notification deadline for the residents we hold data on? Public company: is the SEC four-business-day materiality process documented?

Red flag: missed compliance deadline, failed audit, or a breach nobody logged.



8. ROI VERIFICATION

Question: Are security tools delivering promised value?

What to review:

- Incidents prevented vs. cost of tools
- Time saved by automation and tools
- Employee satisfaction with security tools
- Cyber insurance: do we have it, what does it cover, and would it cover a cross-border incident?

Red flag: expensive tools that nobody uses or understands.

BOTH COUNTRIES

One benchmark for the insurance question. Statistics Canada found only 22% of Canadian businesses carry cyber insurance. In NetDiligence's 2025 study of more than 10,000 U.S. and Canadian claims, the average incident at a small or mid-sized company cost about US\$264,000, and insured firms of that size recovered about 69% of it from their policy. If the answer to "are we insured" is no, it belongs on next week's action list.

WEEKLY COMPLETION

Week of: _____

Reviewed by: _____

Score (items completed out of 8): _____

Action items for next week:

1. _____
2. _____
3. _____

© Elliptic Systems Corporation | EllipticSystems.com. Canadian edition prepared September 2026. Educational material, not legal advice; requirements in both countries change and this checklist will need updating.



WHEN TO ESCALATE

Quick Decision Tree for Security Concerns *United States and Canada edition*

GREEN: MONITOR AND DOCUMENT

Handle through normal channels. Examples:

- Single failed login attempt
- Routine password reset request
- Known software update available
- General security awareness question

Action: document and monitor; no immediate escalation needed.

YELLOW: INVESTIGATE TODAY

Review within business hours. Examples:

- Multiple failed login attempts (3+ in a short time)
- Employee reports a suspicious email
- Unusual data access pattern
- Unapproved AI tool detected in use
- Policy exception request
- Personal information sent across the border (US to Canada or Canada to US) without the privacy check

Action: investigate the same day, document findings, escalate if concerning.

ORANGE: ESCALATE WITHIN 2 HOURS

Potential incident requiring leadership attention. Examples:

- Confirmed phishing email clicked
- Confidential data uploaded to an unapproved AI tool
- Former employee account still active
- Failed security audit finding
- Vendor service outage affecting operations
- Multiple employees reporting the same suspicious activity
- Invoice, banking-change or payment request that turned out to be fake, whether or not money moved

Action:

- Notify the IT/Security Lead immediately
- Notify the department head or manager
- Begin documentation
- Do NOT delete or modify evidence

RED: IMMEDIATE ESCALATION

Active security incident. Respond immediately. Examples:

- Confirmed data breach or unauthorized access
- Ransomware or malware infection



- System compromise detected
- Confidential or Restricted data publicly exposed
- Regulatory violation discovered
- Vendor reporting a security incident affecting your data

Action: 3-STEP BREACH RESPONSE

STEP 1: CONTAIN (first 15 minutes)

- Isolate affected systems (disconnect from the network if needed)
- Preserve evidence; do NOT delete anything
- Stop the spread; prevent further access

STEP 2: NOTIFY (within 30 minutes)

- Call the IT/Security Lead: [phone number]
- Notify the Executive Sponsor: [phone number]
- Contact Legal and the Privacy Officer if personal information may be involved: [phone number]
- Call the cyber insurance claims line: [phone number] (most policies require notice before you hire responders)
- If after hours: [emergency contact info]

STEP 3: DOCUMENT (immediately)

- What happened and when it was discovered
- What systems and data were affected, and whose data (US residents, Canadian residents, which provinces and states)
- Who has been notified
- What containment actions were taken

CANADA

Step 3 is also your legal record. PIPEDA requires a record of every breach of security safeguards, whether or not it was reported, kept for at least 24 months. Include the date discovered, what happened, what data and how many people, the harm assessment, and who was notified.

STEP 4: REPORT TO REGULATORS (Incident Lead, Privacy Officer and Legal, within the first day)

If personal information may be involved, decide within the first day whether the incident creates a real risk of significant harm to individuals. If it does, each country's duties apply separately to the residents of that country, and both clocks run at once.

CANADA

Canada. Report to the Office of the Privacy Commissioner of Canada (priv.gc.ca, online breach report form; 1-800-282-1376) as soon as feasible. Alberta: also the Alberta Commissioner (mandatory). Quebec: also the Commission d'accès à l'information. BC: notify individuals; reporting to the BC OIPC is voluntary today but recommended. Notify affected individuals directly and any organization that can reduce the harm (bank, payment processor, client). Report the cyber incident to the Canadian Centre for Cyber Security (cyber.gc.ca), and fraud or extortion to the Canadian Anti-Fraud Centre (1-888-495-8501) and local police. Designated operators under the Critical Cyber Systems Protection Act (finance, telecom, energy, transportation) report to the Cyber Centre under that Act's timelines.

**UNITED STATES**

United States. Notify affected residents, and in most states the state attorney general, under the breach-notification law of every state where affected people live; all 50 states have one, most set a 30- to 60-day outer limit, and several require notice "without unreasonable delay" or faster (some as short as 30 days, with attorney-general notice thresholds that vary). HIPAA: notify HHS within 60 days (annually for breaches under 500 people) and the media for breaches over 500 in a state. Report the incident to CISA (cisa.gov/report) and the FBI IC3 (ic3.gov). Publicly traded companies: assess SEC Form 8-K materiality within four business days of determining materiality.

BOTH COUNTRIES

Penalties, for the leadership conversation. Canada: knowingly failing to report or record a breach is a PIPEDA offence with fines up to CA\$100,000 per violation; Quebec Law 25 administrative penalties run up to the greater of CA\$10 million or 2% of worldwide turnover, and penal fines up to the greater of CA\$25 million or 4%. United States: state attorneys general fine per violation or per affected resident (often US\$100 to US\$750 each, capped in some states); HHS civil penalties for HIPAA breaches are tiered up to US\$2 million-plus per year per violation category; the FTC can pursue unfair or deceptive practice claims; and class actions follow large breaches in both countries.

EMERGENCY CONTACTS**During business hours**

IT/Security Lead: _____

Executive Sponsor: _____

Legal/Compliance: _____

Privacy Officer: _____

After hours/weekends

Emergency security line: _____

On-call manager: _____

External partners

Elliptic Systems: (425) 357-6222 _____

Cyber insurance 24-hour claims line: _____

Outside counsel (Canada): _____

Outside counsel (US): _____

Regulators and agencies

Purpose	Canada	United States
Privacy breach report	Office of the Privacy Commissioner of Canada, priv.gc.ca , 1-800-282-1376; Alberta OIPC; Quebec CAI; BC OIPC	State attorney general for each affected state; HHS OCR for HIPAA
Cyber incident	Canadian Centre for Cyber Security, cyber.gc.ca	CISA, cisa.gov/report ; FBI IC3, ic3.gov
Fraud, phishing, extortion	Canadian Anti-Fraud Centre, 1-888-495-8501; local police	FBI IC3; FTC, reportfraud.ftc.gov ; local police

Provincial or state regulator specific to our industry: _____



REMEMBER

- Quick reporting saves money. Minutes matter in security incidents.
- You will not be punished for honest mistakes reported promptly.
- Better to over-report than under-report.
- Do not try to "fix it yourself" if it is Orange or Red.
- Preserve evidence; do not delete anything.
- If the data belongs to people in both countries, both sets of rules apply. Tell both regulators.

This card is your quick reference. Keep it visible. For full policies, see: [Company intranet/wiki URL]

© Elliptic Systems Corporation | EllipticSystems.com. Canadian edition prepared September 2026. Educational material, not legal advice. Reporting deadlines and penalties in both countries change; confirm current requirements with your legal advisor.