



AI Data Classification and Access Matrix

A worksheet for defining what information AI may access, restrict, retain, or escalate.

STRUCTURE - CLARITY - BETTER DECISIONS

Practical architecture for accountable AI-enabled work.

What this template is for

Map data classes, permitted use, restricted sources, role-based access, retention, expiry, and review rules before AI systems connect to operational context. Use this guide to make the operating choice explicit, test it with evidence, and record who owns the next decision.

BEST USED WHEN

CRM, HR, finance, document systems, and inbox-connected assistants.

WHO SHOULD BE IN THE ROOM

Include the workflow owner, a person who performs the work, a reviewer with authority to approve or stop it, and the relevant data or tool owner.

CANADIAN CONTEXT

Confirm applicable federal, provincial, territorial, sector, professional, contractual, accessibility, and bilingual-service requirements. Use this workbook as operational preparation, not legal advice.

A five-step working rhythm

01

Public

Which sources can AI use freely?

02

Internal

Which sources are safe only inside the organization?

03

Confidential

Which sources require role, purpose, or approval constraints?

04

Sensitive

Which personal, financial, or regulated data needs strict handling?

05

Forbidden

Which data should never enter this AI workflow?

Build the working record

Complete one record for one workflow. Write enough to support a decision, not a generic technology wish list.

PROMPT	YOUR WORKING NOTES
01 System or workflow	
02 Sensitive data class	
03 Access owner	
04 Public	
05 Internal	
06 Confidential	
07 Decision, owner, evidence, and review date	

Classify client discovery data

STARTING FRICTION

Engagement notes, public case studies, and internal methods need different sharing rules.

WORKFLOW MAP



AI-SUPPORTED ROLE

Propose classifications and access paths from documented rules; flag uncertain or sensitive records. Flag uncertainty around public.

HUMAN AUTHORITY

Data stewards approve classifications, permissions, retention, and prohibited uses. Resolve the public question for this case.

PILOT MEASURE

Track misclassified records, excessive access, denied requests, and cleanup time. Record public exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Separate operating and personal data

STARTING FRICTION

Product and sales trends may be useful while payment and employee details should stay out of the assistant.

WORKFLOW MAP



AI-SUPPORTED ROLE

Propose classifications and access paths from documented rules; flag uncertain or sensitive records. Flag uncertainty around internal.

HUMAN AUTHORITY

Data stewards approve classifications, permissions, retention, and prohibited uses. Resolve the internal question for this case.

PILOT MEASURE

Track misclassified records, excessive access, denied requests, and cleanup time. Record internal exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Classify client files

STARTING FRICTION

A workflow must distinguish public guidance, firm procedures, and client-confidential records.

WORKFLOW MAP



AI-SUPPORTED ROLE

Propose classifications and access paths from documented rules; flag uncertain or sensitive records. Flag uncertainty around confidential.

HUMAN AUTHORITY

Data stewards approve classifications, permissions, retention, and prohibited uses. Resolve the confidential question for this case.

PILOT MEASURE

Track misclassified records, excessive access, denied requests, and cleanup time. Record confidential exceptions separately.

DISCUSSION PROMPT

What evidence would the reviewer need to trust, correct, reject, or escalate this output?

Before the pilot grows

Use these prompts to test whether the proposed workflow can operate responsibly in its Canadian business context.

01

Public

Data classes are named before connection. Name the owner and the operating decision before selecting a tool.

02

Internal

Access rules are role-aware. Record the approved sources, permissions, and missing information.

03

Confidential

Restricted sources are explicit. Test this boundary with representative and adverse cases.

04

Sensitive

Retention and expiry are visible. Preserve review, escalation, and correction evidence.

05

Forbidden

Review or legal escalation is defined. Set a measurable stop condition and the next review date.

06

Readiness to proceed

Context boundaries only work when data classes are visible. AI access should be governed before retrieval feels convenient.

CANADIAN REFERENCE POINTS

Office of the Privacy Commissioner of Canada - Privacy and artificial intelligence
priv.gc.ca/en/privacy-topics/technology/artificial-intelligence/

Government of Canada - Artificial Intelligence guidance, principles, and policy
canada.ca/en/services/science/innovation/artificial-intelligence.html

General operational guidance only. Confirm applicable legal, privacy, cybersecurity, professional, contractual, and regulatory requirements with qualified advisors.