FEBRUARY 2026

Privacy Breach Readiness, Detection, and Response Playbook

For Ontario Provincial Institutions (FIPPA) and Municipal Institutions (MFIPPA)

Prepared by Managed Privacy Canada

Based on 'Privacy Breaches Guidelines for Public Sector Organizations' by the Information and Privacy Commissioner (IPC) Ontario

The **Information and Privacy Commissioner (IPC) of Ontario** is an independent office that promotes open government and protects personal privacy. They oversee Ontario's laws regarding the collection, use, and disclosure of personal information, ensuring that individuals' access and privacy rights are respected.

Scope and exclusions

Use this playbook for public-sector "personal information" breaches under FIPPA (mandatory) and MFIPPA (strong best practice). It is not the IPC's health-sector breach guide and does not replace sector-specific requirements (e.g., PHIPA; CYFSA Part X; FIPPA Part III.1 data integration units).

What is a privacy breach?

A privacy breach occurs when personal information is stolen, lost, accessed, used, disclosed, retained, or disposed of in ways that don't comply with Ontario's privacy laws.

Roles: "Who does what"

The IPC expects institutions to have a documented breach plan that clearly states who does what, who to contact (and backups), and to practice the plan.

Use these standard roles (adapt titles to your organization):

A. Privacy Officer / FOI & Privacy Coordinator (Breach Lead)

Accountable for coordinating the response.

Must:

- Activate the breach response team and open a breach file.
- Ensure assessment/containment begins immediately.
- Lead the RROSH determination (with IT/Program/Legal input).
- Oversee notification content and method (direct vs indirect) and timing ("as soon as feasible").
- Oversee IPC reporting (do not delay because details are incomplete).
- Ensure documentation, remediation tracking, and annual reporting where required.

B. IT / Cybersecurity Lead (Containment + Forensics)

Must:

- Identify affected systems, dates, and suspected compromise window.
- Stop ongoing access/exfiltration; reset credentials; isolate systems; preserve logs and evidence.
- Confirm whether data was accessed, encrypted, exfiltrated, posted online, etc. (needed for notices).

C. Program Owner / Business Lead (Impact + Data Context)

Must:

- Confirm what data elements were involved and the affected population.
- Provide context that affects sensitivity and harm (e.g., vulnerable groups, safety risks).

D. Communications Lead (Public-facing messaging)

Must:

- Draft public statements and FAQs aligned with the notification plan (especially if indirect notice is used or large numbers are affected).

E. HR / Labour Relations (Workforce-related breaches)

Must:

- Handle internal misconduct (e.g., snooping), access suspensions, discipline, and training follow-ups. The IPC flags suspending access rights in staff-access incidents pending investigation.

F. Legal Counsel (Privilege + legal constraints)

Must:

- Advise on legal prohibitions (note: where notifying individuals is prohibited by law, FIPPA institutions may still need to report to the IPC).
- Advise on coordination with law enforcement and regulatory bodies.

G. Vendor / Procurement Lead (Third-party breaches)

Must:

- Ensure contracts require vendors to notify the institution immediately of a breach (the institution remains primarily responsible for notifying individuals if RROSH is met).

H. Executive Sponsor (ADM/CAO/Clerk/Commissioner)

Must:

- Confirm resourcing, risk posture, and approve notification/public communications where needed.

Phase 1: Prepare

Readiness Checklist (Check all that apply, then date and save the completed form)

Governance & People

- [ ] Named Breach Lead (Privacy Officer/FOI Coordinator) and alternate.
- [ ] Breach response team roster (IT, Legal, Comms, HR, Program, vendor contacts).
- [ ] Current escalation tree (24/7 contact method, backups).
- [ ] Tabletop exercise completed in last 12 months; lessons logged.

Process & Tools

- [ ] Standard forms/templates ready:
  - Intake/triage form … Completed checklist in Phase 2
  - RROSH worksheet … Completed checklist in Phase 3
  - Notification templates (direct + indirect) … Completed checklist in Phase 4
  - IPC reporting package checklist … Completed checklist in Phase 5
  - Investigation report outline … Completed checklist in Phase 6
  - Remediation plan tracker … Completed checklist in Phase 7
- [ ] Evidence preservation procedure (logs, emails, tickets, vendor notices).

Prevention (IPC “privacy management program” expectation)

- [ ] Leadership oversight and designated privacy officer.
- [ ] Staff training, clear policies, disciplinary measures.
- [ ] Technical safeguards; audits/access reviews; retention controls; vendor oversight.

Phase 2: Identify, Assess, and Contain

Triage Checklist (first hours)

Identify

Open a breach file (unique ID; time discovered; reporter; system).

Assess scope (preliminary)

- [ ] What personal information is likely involved and its nature?
- [ ] How much information was exposed?
- [ ] How many people may be affected and who are they?
- [ ] Which systems were/may be compromised and when?

Contain

- [ ] Leadership oversight and designated privacy officer.
- [ ] Staff training, clear policies, disciplinary measures.
- [ ] Technical safeguards; audits/access reviews; retention controls; vendor oversight.

Rule: Don't wait for a full investigation to start containment—IPC expects a preliminary assessment "as soon as possible" to determine next steps (including reporting/notification).

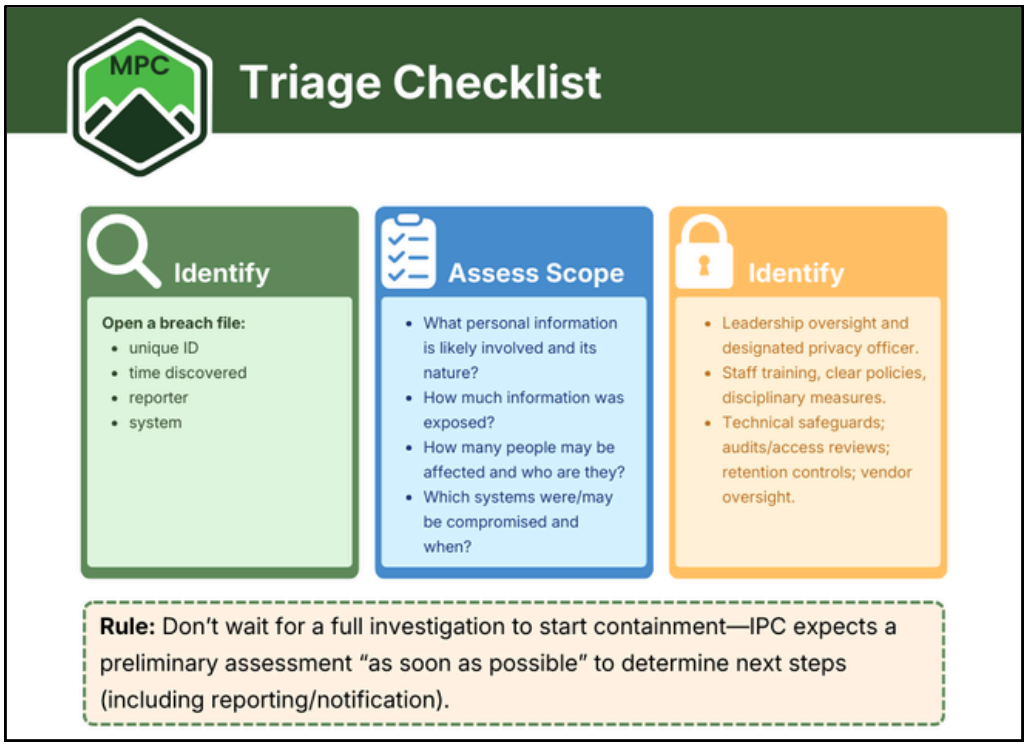

Figure 1. Triage Checklist Visual: Identify from Assess, and Contain, Privacy Breach Readiness, Detection, and Response Playbook (Managed Privacy Canada)

Phase 3: RROSH Decision

RROSH Questionnaire (complete for every breach)

Institutions must determine whether the breach creates a real risk of significant harm (RROSH). The IPC lists core factors and explains that not all factors must be satisfied and other factors may be relevant.

Sensitivity of personal information

- [ ] What types of personal information were impacted?
- [ ] Could compromise cause significant harm (identity theft, financial loss, humiliation, reputational damage, etc.)?
- [ ] Context increases sensitivity? (e.g., vulnerable individuals; safety concerns; disciplinary records; geolocation).
- [ ] More data elements together increase sensitivity (e.g., name + DOB + address + financial).
- [ ] Could exposed elements be combined with publicly available info to cause harm?

Probability of misuse

- [ ] Who obtained/likely obtained the info (unknown attacker, vendor, misdirected recipient, internal staff)?
- [ ] Was it accessed, exfiltrated, posted, sold, or merely exposed? (use IT findings).
- [ ] Is there evidence of actual misuse (fraud reports, account takeover, dark web posting)?

Ability of individuals to reduce risk / mitigate harm

- [ ] Are there practical steps individuals can take now (credit monitoring, password reset, bank contact)?
- [ ] Can the institution do something to reduce risk (forced resets, token revocation, account flags)?

Bottom-line determination

- [ ] Based on A–C, is it reasonable to believe there is a real risk of significant harm?

I**f YES (RROSH met):** proceed to notify individuals and report to IPC “as soon as feasible.”
If NO: document rationale; consider voluntary notice where appropriate; still investigate and remediate.

E. Visual Component

Below is a visual illustration of the RROSH Decision Questionnaire from the previous page.

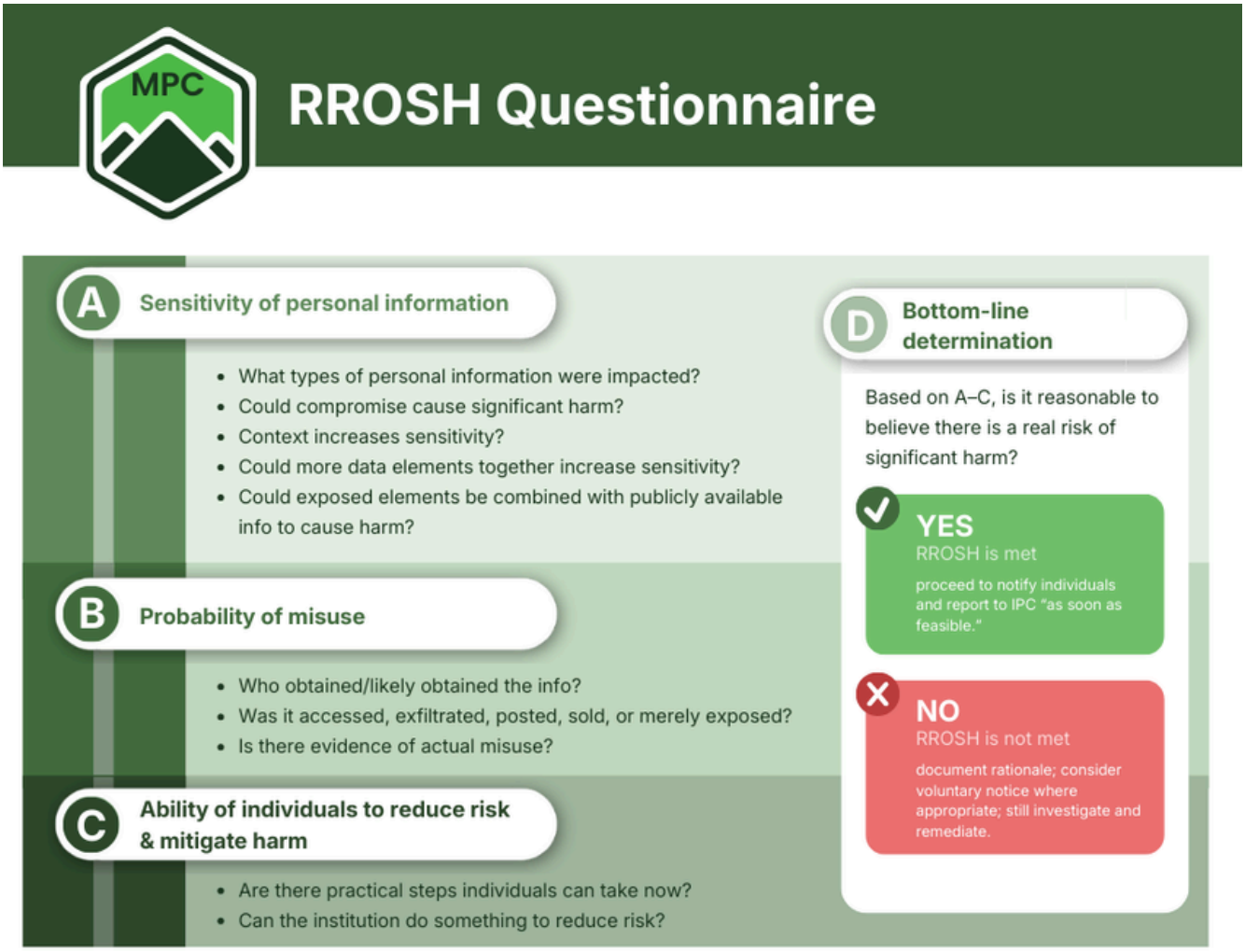

Figure 2. RROSH Decision Questionnaire from Privacy Breach Readiness, Detection, and Response Playbook (Managed Privacy Canada)

Phase 4: Notification Template Checklist

A. Timing

- [ ] Notify as soon as feasible following a breach.
- [ ] If law enforcement is involved, advise them of notification plans.

Method selection (Direct vs Indirect)

ect notice is preferred

irect notice may be used only in specific situations, including (non-exhaustive):

- [ ] Unable to determine identities despite reasonable steps.
- [ ] Contact information reliability issues (may require hybrid approach).
- [ ] Direct notice would unreasonably and significantly interfere with operations.
- [ ] Direct notice likely harmful/detrimental (distress/safety risk).
- [ ] Very large number of individuals (impractical) with context considered.
- [ ] For voluntary notifications where RROSH not met and risk is low.

ıdirect notice is used:

- [ ] Use methods reasonably expected to reach affected individuals; multiple methods are best practice (website notice, posters, newspapers, social media, radio/TV, news releases, town halls/webinars).

Notice content checklist (must be plain language)

- [ ] Direct and indirect notifications should include the following items (use as a strict checklist):
- [ ] Date of notice.
- [ ] Statement that the individual may complain to the IPC + how to do so (mandatory for FIPPA notices under s. 40.1(4) when provided in accordance with that section).
- [ ] Statement that the complaint must be filed within one year (FIPPA s. 40.1(4) notices only).
- [ ] IPC mailing address: 2 Bloor Street East, Suite 1400, Toronto, ON M4W 1A8.
- [ ] Enough information to understand impact; circumstances; cause (if known).
- [ ] Date/period of breach; date your institution became aware.
- [ ] Description of personal information affected (as much detail as possible).
- [ ] How the information was affected (accessed/encrypted/exfiltrated/posted, etc.).

- [ ] Any known risk of harm.
- [ ] Steps your institution took to contain and reduce/mitigate harm.
- [ ] Steps individuals can take to protect themselves (bank contact; monitor statements; obtain credit report, etc.).
- [ ] Statement whether you reported to IPC and other regulators, if applicable.
- [ ] Institutional contact person information for questions and help.

Phase 5: IPC Reporting Package Checklist

IPC reporting rules and expectations

- [ ] If it's reasonable to believe there is RROSH, report to the IPC as soon as feasible after determining the breach occurred.
- [ ] For large-scale notifications, the IPC strongly recommends reporting before notifying the public so the IPC can help refine the notification plan.
- [ ] Do not delay reporting because details are incomplete; send updates as you learn more.

"Other authorities" notification prompt (case-by-case)

Consider informing, as applicable:

- [ ] Law enforcement (if theft/crime suspected).
- [ ] Professional/regulatory bodies (professional standards).
- [ ] Technology suppliers (recall/fix).
- [ ] Canadian Centre for Cyber Security (cyber incident).

Phase 6: Investigation Checklist

Your investigation should determine what happened, why, and how to prevent recurrence.

Investigation checklist

- [ ] Timeline: initial intrusion/error → detection → containment → recovery.
- [ ] Cause: human error, technical failure, vendor failure, malicious insider, external attacker.
- [ ] Scope confirmation: data elements, affected individuals count, duration of exposure.
- [ ] Safeguards assessment: access controls, logging, encryption, retention compliance, training adequacy.
- [ ] IPC cooperation readiness: institutions have a duty to cooperate and assist IPC reviews/investigations.

Phase 7: Remediation Checklist

The IPC expects prevention via privacy management and remediation; breaches often reveal weaknesses that must be promptly addressed.

Reduce Future Risk (mandatory follow-through)

- [ ] Limit access privileges; retire legacy systems; monitor/audit systems with personal information.
- [ ] Strong/MFA authentication; vulnerability management; endpoint protection; backups; encryption.
- [ ] Incident response planning; threat-risk assessments for new technologies.
- [ ] Confirm retention schedules (don't retain longer than necessary).
- [ ] Regular audits of employee access; privacy warning flags on systems.
- [ ] Strong procurement practices and third-party controls.

Phase 8: Recordkeeping and Annual Reporting (FIPPA)

Recordkeeping

- [ ] Maintain a record of the total number of RROSH breaches reported to the IPC.
- [ ] Keep enough detail to defend your RROSH decision and show steps taken.

Annual reporting (FIPPA institutions)

- [ ] Submit annual breach statistics to IPC by March 31 of the following year.
- [ ] Annual report must include:
  - number and type of reported breaches; and
  - number of individuals affected by each breach.

TTX / Privacy Breach Simulation Scenario Pack

How to use this scenario pack

60–90 minutes per scenario
Participants: Privacy/FOI, IT, Program, Comms, Legal, HR (as needed), Vendor lead
Materials: RROSH worksheet; Notice content checklist; IPC reporting checklist; Breach log; Remediation tracker

Rules:

1. Treat each scenario as real and time-sensitive.
2. Make decisions using the organization's actual tools and escalation paths.
3. Document as you go (your documentation is part of the exercise outcome).
4. At each decision point, the facilitator asks: "What do you do now, who does it, and what do you record?"

Misdirected Email with Attachment
Scenario: An employee emails a spreadsheet containing personal information to the wrong external recipient.

Lost Laptop/USB
Scenario: A laptop or USB containing program files with personal information is lost on public transit, and it is unclear whether the device was encrypted.

"Snooping" / Unauthorized Staff Access
Scenario: Audit logs show an employee repeatedly accessing a neighbour's (or acquaintance's) file without a business reason.

Vendor Breach
Scenario: A service provider alerts you to suspicious activity affecting a system that stores or processes your institution's personal information.

Ransomware
Scenario: Multiple systems are encrypted and the attacker claims personal information was copied out before encryption.

Large-scale Mailing Error
Scenario: Thousands of recipients receive mailed packages containing someone else's personal information due to a print/insert error.

Shared Drive / Cloud Misconfiguration
Scenario: A shared folder containing personal information was misconfigured and accessible beyond the intended audience (staff-wide or publicly) for an unknown period.

High-Risk Safety Context
Scenario: Personal information tied to safety-sensitive services (e.g., shelter locations, witness-related information) is exposed, and direct notice could increase risk to individuals.