[REDACT]LABS

RESOURCE / 03

PRIVACY COMPLIANCE

PIPEDA Breach Response Playbook Template

A workable template for Canadian organizations subject to PIPEDA's mandatory breach notification requirements, with the OPC's published criteria built in.

TORONTO, ON / 2026

redactlabs.ca

Why this matters

Since November 1, 2018, every private-sector organization in Canada subject to PIPEDA has had a legal duty to: report breaches of security safeguards involving personal information that pose a “real risk of significant harm” to the Office of the Privacy Commissioner of Canada (OPC); notify affected individuals; and maintain a record of all breaches regardless of risk level for 24 months.

The penalty for knowingly contravening reporting and notification requirements is a fine of up to $100,000 per violation. More important than the fine is the reputational consequence of a breach discovered to have been unreported.

This playbook is a template. Customize the bracketed placeholders with your organization’s contacts and systems.

> DISCLAIMER
>
> This template is for general informational purposes and does not constitute legal advice. Engage privacy counsel before responding to a real incident. The OPC publishes authoritative guidance at priv.gc.ca that should always take precedence over this template.

Roles and contacts

Fill in named individuals and contact channels before an incident, not during one.

Incident response coordinator

Name: [NAMED] · Phone: [NUMBER] · Email: [EMAIL] · Backup: [NAMED]

Privacy officer

Name: [NAMED] · Phone: [NUMBER] · Email: [EMAIL]

External counsel

Firm: [FIRM] · Lead: [NAMED] · Phone: [NUMBER]

Cyber insurance carrier

Carrier: [CARRIER] · Policy: [NUMBER] · Claims hotline: [NUMBER] · Notify within: [X HOURS]

External technical support

Provider: [FIRM] · Lead: [NAMED] · Phone: [NUMBER]

Board chair (for material incidents)

Name: [NAMED] · Phone: [NUMBER]

Public communications lead

Name: [NAMED] · Phone: [NUMBER]

Phase 1: Detection and triage

First hour

1. The detector notifies the Incident Response Coordinator immediately.
2. The Coordinator opens an incident record: date and time of detection, how detected, who detected, what is suspected, immediate actions taken.
3. The Coordinator engages the Privacy Officer if personal information may be involved.
4. Take immediate containment actions if obvious and safe (disable a compromised account, disconnect an infected device). Document each.
5. Do not wipe systems, restore from backup, or alter logs until you have a confirmed plan. Preserved evidence matters.

First 24 hours

1. Begin scoping: what systems, what data, what individuals, what time window?
2. Engage external technical support if internal expertise is insufficient.
3. Notify cyber insurance carrier per policy requirements (failure to notify within window can void coverage).
4. Begin a written timeline. Update at least daily for the first week.
5. Decide who needs to know inside the organization (need-to-know basis).

Phase 2: Real-risk-of-significant-harm assessment

PIPEDA requires you to determine whether the breach poses a “real risk of significant harm” (RROSH) to any affected individual. The OPC defines “significant harm” as including: bodily harm, humiliation, damage to reputation or relationships, loss of employment / business / professional opportunities, financial loss, identity theft, negative effects on credit record, damage to or loss of property.

The OPC’s published factors for assessing whether the risk is “real”:

- Sensitivity of the personal information involved.
- Probability that the personal information has been, is being, or will be misused.
- Any other relevant factor.

Sensitivity factors

Higher sensitivity: financial account numbers, government identifiers (SIN, passport, driver’s license), health information, sexual or relationship information, login credentials with associated email/username.

Lower sensitivity: name and email alone (in most contexts), publicly available information.

Probability factors

Higher probability of misuse: information was deliberately taken; taken by a known malicious actor; appeared on the dark web; in a format easily monetized.

Lower probability: disclosed to a known, trusted recipient who has confirmed deletion; technical safeguards (intact encryption keys) make misuse impractical; information was not actually accessed.

> DOCUMENT THE ASSESSMENT
>
> Whether or not you conclude RROSH applies, write down your reasoning. The OPC may ask. The reasoning is more important than the conclusion.

Phase 3: Reporting and notification

If RROSH applies, two notifications are required:

Notification to the OPC

Make the report as soon as feasible after determining the breach has occurred. Use the OPC's online form at priv.gc.ca. Include:

- Description of circumstances and cause.
- Day or time period of the breach.
- Description of the personal information involved.
- Estimate of the number of individuals affected.
- Steps taken to reduce or mitigate risk of harm.
- Steps taken or planned to notify affected individuals.
- Name and contact for someone who can answer the OPC's questions.

Notification to affected individuals

Also as soon as feasible. Must contain enough information for the individual to understand the significance and take steps to reduce harm:

- Description of circumstances.
- Day or time period.
- Description of the personal information involved.
- Steps the organization has taken.
- Steps the individual could take.
- Contact information for someone who can answer questions.
- How to make a complaint to the OPC.

Direct vs. indirect notification

Direct notification (email, letter, phone) is the default. Indirect (public posting, advertisement) is only acceptable when: direct would cause further harm; cost is prohibitive; the organization does not have current contact information.

Phase 4: Notification to other organizations

If another organization (a credit bureau, payment processor, partner) can take steps to reduce the risk of harm, you may also be required to notify them.

Phase 5: Record-keeping

You must maintain a record of every breach of security safeguards involving personal information, regardless of whether it triggers reporting obligations. Records must be retained for 24 months after the day on which the organization determined the breach occurred. The OPC may request these records at any time.

The record should include: date or estimated date of the breach, general description of circumstances, nature of information involved, RROSH assessment with reasoning, actions taken in response.

Phase 6: Post-incident review

Within 30 days of incident closure, conduct a written post-incident review. Cover: what happened, what worked in response, what did not, changes needed (technical, procedural, policy, training), and who is responsible for each change with a target date. Bring to board if material.

Review questions

- How was the breach detected? Could it have been detected earlier?
- How long was the gap between detection and containment?
- Were all the right people notified internally? In time?
- Were external parties (counsel, insurance, OPC) notified per the playbook?
- Were affected individuals notified clearly and helpfully?
- What controls would have prevented this incident?
- What playbook changes are needed?

Cross-jurisdictional considerations

Quebec Law 25

If any affected individuals are Quebec residents, Quebec Law 25 also applies. Law 25 uses “risk of serious injury” rather than PIPEDA’s “real risk of significant harm” — the thresholds are similar but not identical, and Quebec requires notification to the Commission d’accès à l’information (CAI) on essentially the same trigger.

Provincial health privacy law (PHIPA, etc.)

If the breach involves personal health information and you are a health information custodian under provincial law (PHIPA in Ontario, equivalent statutes elsewhere), additional notification obligations apply to the relevant provincial Information and Privacy Commissioner.

Foreign jurisdictions

If affected individuals reside outside Canada, that jurisdiction’s privacy law may apply. GDPR (EU), CCPA (California), and other regimes have their own breach notification windows and content requirements.

Sources

The authoritative source for PIPEDA breach reporting requirements is the Office of the Privacy Commissioner of Canada at priv.gc.ca. The OPC publishes the official breach reporting form, detailed guidance on assessing real risk of significant harm, and recordkeeping requirements. Quebec Law 25 guidance is published by the Commission d’accès à l’information du Québec at cai.gouv.qc.ca. Ontario PHIPA guidance is published by the Information and Privacy Commissioner of Ontario at ipc.on.ca.

If you want help

Our charity and SMB engagements include breach response readiness as a standard component. We help inventory, write the playbook, train staff, and stand up the operational pieces (incident channels, evidence preservation, communication templates) before an incident.

contact@redactlabs.ca