

DOCUMENT 3 OF 4 · PRIVACY RULES AND INSURER QUESTIONS

Rules and Insurance Briefing

Your findings beside the privacy and sector rules that apply, and the insurer questions an outside read can answer.

PREPARED FOR

Harbourview Law LLP

DATE OF ASSESSMENT

15 Sep 2026

DOMAIN ASSESSED

harbourview-llp.example

REFERENCE

LT-BIZ-2026-7098

IN THIS DOCUMENT

1	The rules that apply to you	p. 2
2	Each finding and the rule it touches	p. 3
3	Questions insurers ask at renewal	p. 4
4	What to keep on file	p. 6

THREE DOCUMENTS AND A DATED RECORD

1 Owner Summary

2 Technical Evidence

3 Rules and Insurance

4 Assessment Record

SECTION 1 · THE RULES THAT APPLY TO YOU

Two rules, in plain words

PIPEDA, Principle 4.7 · Safeguards

Personal information must be protected by security safeguards appropriate to its sensitivity.

Applies to organizations that handle personal information in the course of commercial activity.

Source: PIPEDA, S.C. 2000, c. 5, Schedule 1, cl. 4.7

PIPEDA, s. 10.1 and 10.3 · Breaches

Report a breach of security safeguards that creates a real risk of significant harm to the Privacy Commissioner as soon as feasible, and keep a record of every breach of security safeguards for 24 months.

Applies whenever personal information under your control is involved.

Source: PIPEDA s. 10.1, s. 10.3; Breach of Security Safeguards Regulations, SOR/2018-64, s. 6(1)

What the statute says about penalties. PIPEDA, S.C. 2000, c. 5, s. 28: "Every organization that knowingly contravenes subsection 8(8), section 10.1 or subsection 10.3(1) or 27.1(1) or that obstructs the Commissioner ... is guilty of (a) an offence punishable on summary conviction and liable to a fine not exceeding \$10,000; or (b) an indictable offence and liable to a fine not exceeding \$100,000." Only a knowing contravention is an offence. Prosecution is by the federal Crown; the Privacy Commissioner says it does not prosecute offences or issue fines. Text read on 15 October 2026.

SECTION 2 · MAPPING

Each finding and the rule it touches

FINDING	RULE IT TOUCHES	WHAT THE RULE ASKS, AND WHAT TO KEEP ON FILE
F-01 Firm addresses in breach data HIGH	PIPEDA Principle 4.7	Personal information must be protected by security safeguards appropriate to its sensitivity. Keep on file: Confirmation of each password reset and of multifactor sign-in set to Enforced, dated. Source: PIPEDA, S.C. 2000, c. 5, Schedule 1, cl. 4.7
F-02, F-03, F-04, F-05, F-06, F-07, F-08, F-09 No DMARC record; Your site is missing 6 browser protections; DNSSEC not enabled; Your robots.txt file publicly lists internal paths (/wp-admin/); and 4 more HIGH	PIPEDA Principle 4.7	Personal information must be protected by security safeguards appropriate to its sensitivity. Keep on file: The result of the reproduce command after the fix, dated. Source: PIPEDA, S.C. 2000, c. 5, Schedule 1, cl. 4.7
F-01 If an exposed account was used by someone else HIGH	PIPEDA s. 10.1 and 10.3	Report a breach of security safeguards that creates a real risk of significant harm to the Privacy Commissioner as soon as feasible, and keep a record of every breach of security safeguards for 24 months. Keep on file: A breach-record entry for any account found to have been used, even if you conclude no breach of your safeguards occurred. Source: PIPEDA s. 10.1, s. 10.3; Breach of Security Safeguards Regulations, SOR/2018-64, s. 6(1)

SECTION 3 · AT RENEWAL

Questions cyber insurers commonly ask, and your answer today

Each answer comes from what we could check from outside, with the evidence behind it, to help you fill in the application. Questions no outside check can see are marked Not visible: answer those from inside your firm. The insurer makes its own decision.

QUESTION	YOUR ANSWER TODAY	SEE
Do you publish an SPF record listing the servers allowed to send your mail? SPF record published and ending in -all: v=spf1 include:spf.protection.outlook.com -all. Helps you answer: Answer Yes and quote the record.	YES	
Is outgoing email signed with DKIM? DKIM signing couldn't be confirmed from outside (default, selector1, selector2, google, s1, s2, k1, mxvault). A key on another name is not visible from outside. Helps you answer: Check which selector your mail service signs with. If none, turn DKIM signing on in the mail service.	NOT CONFIRMED	
Does your domain enforce DMARC at quarantine or reject? No DMARC record is published for harbourview-llp.example, so mail forged in its name is not refused. Helps you answer: Answer No today. One DNS record at p=reject turns this to Yes.	NOT YET	F-02
Do you require multi-factor sign-in for email and remote access? Whether a second sign-in step is enforced cannot be seen from outside. What we did see that it applies to: a WordPress administrator sign-in. Helps you answer: Confirm that each sign-in listed here requires a second step, then answer for your firm.	NOT VISIBLE	

Table continues on the next page

QUESTION	YOUR ANSWER TODAY	SEE
Do you keep internet-facing software patched and up to date? No known-vulnerable website software found in the scripts we read. The server names its software (nginx), which helps an attacker match known flaws. Helps you answer: Answer Yes for the website software we read; hiding the version banner closes the rest.	PARTLY	F-04
Is all web traffic to your site encrypted with a valid certificate? Valid certificate from Let's Encrypt, expires Dec 06 20:43:20 2026 GMT. The site does not yet insist on a secure connection (no HSTS). Helps you answer: Answer Yes; adding the HSTS header makes it complete.	PARTLY	
Are remote-access and database services closed to the internet? No remote-access or database port answered from outside (2 ports checked open, none of them remote access). Helps you answer: Answer Yes for what faces the internet.	YES	
Are staff email addresses clear of known breach data? No firm address at harbourview-llp.example was found in monitored breach databases. Helps you answer: Answer Yes.	YES	
Do you keep offline or immutable backups, and test restoring them? Not visible from outside: no outside check can see this. Helps you answer: Answer from inside your firm.	NOT VISIBLE	
Is sensitive data encrypted on laptops and servers? Not visible from outside: no outside check can see this. Helps you answer: Answer from inside your firm.	NOT VISIBLE	
Do you run endpoint protection (EDR) on every computer? Not visible from outside: no outside check can see this. Helps you answer: Answer from inside your firm.	NOT VISIBLE	

Source for the question set: common items in Canadian and US cyber insurance applications. Wording varies by insurer.

SECTION 4 · WHAT TO KEEP ON FILE

Four things that show you acted

☐	Set your email to reject forged mail: the proof check result, with the date	Date _____
☐	Reset the exposed logins and require a second sign-in step: the proof check result, with the date	Date _____
☐	Breach-record entry for F-01, even if no breach of your safeguards is found	Date _____
☐	This briefing and the Assessment Record of reference LT-BIZ-2026-7098	Date _____

Before you sign an application: an answer of "Yes" to a question marked "Not yet" on page 4 can affect a claim later. Close the item first, or answer as it stands and attach this briefing.

This briefing is not legal or insurance advice, and LeakTrace Inc. is not a law firm. It describes rules and policy terms in general, not how they apply to you, and it does not change any insurance policy. Prepared from an external assessment on 15 Sep 2026. Confirm the position that applies to your organization with your lawyer and your insurance broker.