AltaCom
An Abatri Solutions Inc. Company

The Alberta Law Firm IT Self-Assessment

Fifteen things worth checking in the technology your practice runs on — written for firms that would rather find the gaps themselves than discover them during an incident.

Managed IT · Cybersecurity · Cloud · Web
For professional firms across Alberta

Calgary, Alberta
altacom.ca · 403-744-5411

AltaCom
An Abatri Solutions Inc. Company

HOW TO USE THIS

Read it twice, at two different heights.

Each of the fifteen sections opens with a single statement for whoever signs off on firm decisions, followed by the specific things an office manager or IT provider can actually go and verify. You can read the first part in ten minutes and hand the rest to someone else.

Nothing here requires you to become technical. Every item is phrased as something you can ask for, look at, or request in writing. At the end of each section there is one question to score, and the scorecard near the back collects all fifteen into a single number you can act on.

This self-assessment is deliberately practical rather than exhaustive. It reflects what we see repeatedly in small and mid-sized Alberta practices — not a theoretical maximum.

CONTENTS

01 Technology as a practice management issue

IN ONE LINE

Your regulator already treats technology as part of competence itself — the Code of Conduct expects every lawyer to develop "an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice" (Rule 3.1-2, Commentary [5]).

This reframes the question. Alongside the Code, the Law Society publishes practice management guidance on cloud computing and on remote-work confidentiality. IT spending is not a discretionary overhead line sitting beside the coffee service; the tools you choose are part of how the firm meets its duty of confidentiality. That makes it a partner-level decision, not something delegated entirely downward and reviewed when something breaks.

What to check

- [ ] Someone in the firm has actually read the Law Society's practice management resources on cloud computing and on remote-work confidentiality.
- [ ] One named person is accountable for technology decisions — not "whoever is free."
- [ ] There is a written record of which systems the firm uses and who has access to each.
- [ ] Technology comes up at least annually at a partner or management meeting, with a budget attached.

A NOTE ON SCOPE

This self-assessment is not legal, compliance or insurance advice. Where an item touches your professional obligations, confirm the specifics with the Law Society's Practice and Equity Advisors rather than relying on a document written by your IT provider.

SCORE IT

Is technology owned by a named person, with a documented list of systems, a budget and an annual review?

☐ **0** none of these ☐ **1** some of these ☐ **2** all four

02 Where your client data actually lives

IN ONE LINE

Most firms cannot answer “where is our client data?” in under a minute — and you cannot protect, back up or hand over what you have never mapped.

This is the exercise we would do first, and it is the one most firms skip. It takes an afternoon and it usually produces at least one genuine surprise: an old server nobody decommissioned, a departed articling student’s mailbox still receiving mail, or a partner’s personal cloud drive holding the only copy of something.

What to check

- [ ] List every location matter content sits: mailboxes, document store, practice management system, accounting, personal devices, home computers, USB drives, paper files, off-site storage.
- [ ] For each, note who has access, whether it is backed up, and whether it is encrypted.
- [ ] Identify anything stored outside Alberta or outside Canada — and know your answer before a client asks.
- [ ] Confirm that departed staff, students and contractors no longer have access to any of it — section 03 covers how to make that stick.

RED FLAG

Matter documents that exist only as email attachments and were never filed anywhere else. When that lawyer leaves, the file leaves with them.

SCORE IT

Could you produce a current written map of every place client data lives, and who has access to each?

☐ **0** no ☐ **1** partially ☐ **2** yes, written and current

03 Identity and access

IN ONE LINE

Having multi-factor authentication switched on is not the same as having it enforced — accounts are regularly compromised by routes that never produce a prompt at all.

This is the single most common gap we find, and the most misunderstood. A firm will say with complete sincerity that MFA is enabled, and be right — while older sign-in protocols remain open, a handful of accounts sit on a long-forgotten exemption list, and a stolen session token lets someone in without ever being challenged. The prompt you expected never appears, and neither does the alert.

What to check

- [ ] MFA is enforced through a policy applied to everyone, not switched on per user and hoped for.
- [ ] Legacy authentication protocols are blocked outright.
- [ ] Every exemption and emergency access account is documented and reviewed on a schedule.
- [ ] Administrators use separate accounts from their day-to-day mailbox.
- [ ] Passwords are unique per system and kept in a firm-provided password manager — not reused or in a spreadsheet.
- [ ] Sign-in logs are actually monitored — someone would notice a login from another country.
- [ ] Departures follow a written checklist run the same day: access removed across every system, sessions revoked, devices returned or wiped, and any files held only by that person recovered first.

RED FLAG

An unusual sign-in occurs and nobody in the firm hears about it for weeks — or hears about it only because a client asks why they received a strange email.

SCORE IT

Is MFA enforced for everyone with legacy protocols blocked, sign-in activity monitored, and access removed the same day someone leaves?

- [ ] **0** no or unsure
- [ ] **1** some of these
- [ ] **2** all four, verified

04 Email, phishing and payment fraud

IN ONE LINE

For a law firm the expensive failure is usually not encrypted servers — it is a payment sent to the wrong account on instructions that looked entirely legitimate.

Firms handle other people's money at scheduled, predictable moments. That combination makes conveyancing, settlements and disbursements a standing target. The attack rarely looks like an attack: it arrives mid-thread, in the right tone, often from a real address that has already been compromised.

What to check

- [ ] SPF, DKIM and DMARC are configured and enforced on your domain, not merely present.
- [ ] External senders are visibly marked in the mail client.
- [ ] New mailbox forwarding rules generate an alert to someone who will read it.
- [ ] A written rule: banking or payout instructions are never accepted or changed on the strength of an email — always confirmed by voice, on a number already held on file.
- [ ] Everyone knows the rule applies to instructions that appear to come from a partner.
- [ ] Staff have somewhere to report a suspicious message without feeling foolish.
- [ ] Everyone completes security awareness training on joining and at least annually, and the firm keeps a record of who has done it — insurers ask, and so do some clients.
- [ ] Simulated phishing is run periodically, with reporting rates tracked over time rather than used to catch people out.

THE HABIT THAT WORKS

Callback verification on a previously known number, every time, no exceptions for urgency. Urgency is the pressure the fraud depends on, so treating it as a reason to slow down rather than speed up is the whole defence.

SCORE IT

Do you have email authentication enforced, a written callback rule on payment instructions, and awareness training everyone completes annually?

☐ **0** none ☐ **1** one or two ☐ **2** all three

05 Devices and the security baseline

IN ONE LINE

Every device holding client material should be firm-managed and encrypted — otherwise you are trusting a laptop you cannot see, update or wipe.

The baseline here is unglamorous and largely invisible when it is working. It matters most in the mundane cases: a laptop left in a taxi, a machine handed to a new hire without being rebuilt, an old desktop sold or donated with the drive intact.

What to check

- [ ] Full-disk encryption on every laptop and desktop that touches client data.
- [ ] Operating system and application updates are managed and reported on, not left to individuals.
- [ ] Endpoint protection is installed *and* someone reviews the alerts it raises.
- [ ] Screens lock automatically after a short idle period.
- [ ] Phones that carry firm email are locked, encrypted and remotely wipeable if lost.
- [ ] A clear rule on personal devices — and a technical control behind it, not just a paragraph in a manual.
- [ ] Retired equipment has its drive securely wiped or destroyed, with a record kept.

THE FIVE-MINUTE VERSION

Ask for a single list of every computer the firm owns, showing for each one: who uses it, when it last received updates, and whether the drive is encrypted. If that list cannot be produced within a day, the gap is not the encryption — it is the visibility.

SCORE IT

Are all devices encrypted, centrally managed and patched, with secure disposal recorded?

☐ **0** no ☐ **1** some ☐ **2** all, with evidence

06 Your network and the office itself

IN ONE LINE

The office network is usually the oldest thing in the firm and the least documented — often still running on equipment nobody has logged into since it was installed.

Firewalls and switches are bought once and then forgotten, which is how a firm ends up depending on a device that stopped receiving security updates years ago. The other half of this is physical: reception guest Wi-Fi sharing the same network as the file server, an unlocked server cupboard, a meeting room network port that reaches everything.

What to check

- [ ] A business-grade firewall is in place, still supported by its manufacturer, and receiving firmware updates.
- [ ] Its administrative password is not the factory default, and someone current can log in.
- [ ] Web or DNS filtering is switched on, so known malicious sites are blocked before anyone reaches them — and someone can see what it blocked.
- [ ] Guest and client Wi-Fi is fully separated from the network your firm's systems sit on.
- [ ] Wi-Fi uses modern encryption, and the password changes when someone with it leaves.
- [ ] Any on-premises server is patched, monitored, and physically secured in a locked space.
- [ ] Someone has a current diagram or list of what is on the network, including printers and anything else connected.

RED FLAG

A firewall past its end-of-support date, or one nobody can log in to. Both mean the firm's perimeter is whatever it was configured to be years ago, and no longer reflects who works there or how.

SCORE IT

Is your firewall supported and managed, web filtering on, and guest Wi-Fi separated from firm systems?

☐ **0** no or unsure ☐ **1** some of these ☐ **2** all three, verified

07 Documents, drives and paper

IN ONE LINE

A shared drive organised by whoever happened to create the folder becomes unsearchable within a few years, and a paper room is a confidentiality and continuity risk nobody has budgeted for.

The test we like is simple: ask a lawyer to find a specific document from a matter closed six years ago, and time it. The result tells you more about your document management than any audit. Firms rarely feel this cost as a line item — it surfaces as billable hours quietly lost to searching, and as risk at the moment of a file transfer or a complaint.

What to check

- [ ] Documents are organised by matter, with a naming convention people actually follow.
- [ ] Real version history exists — not filenames ending in *final_v3_revised*.
- [ ] Permissions are set by matter or team where sensitivity requires it, rather than everyone seeing everything by default.
- [ ] A retention and destruction schedule exists, and something enforces it.
- [ ] Email has a retention position and a way to place a litigation hold — mailboxes are records too, and "we just keep everything forever" is a decision with consequences, not the absence of one.
- [ ] Paper has a plan: what gets scanned, by when, and what happens to the originals.
- [ ] Closed files are retrievable by someone other than the lawyer who ran the matter.
- [ ] If the firm operates a trust account, its accounting software appears on the Law Society's current list of approved vendors.

BEFORE YOU CHANGE SYSTEMS

Approval here is narrow but important: the Law Society's Trust Safety department approves accounting software for the purpose of generating the annual Trust Safety Accounting Upload. The list changes, so check the current version rather than relying on a vendor's claim or a colleague's recommendation. Note also that practice management, document management and trust accounting are three different jobs — a product may do one well and another not at all.

SCORE IT

Are documents and email organised and retained, so any authorised person can retrieve a closed file quickly?

☐ **0** no ☐ **1** partially ☐ **2** yes, reliably

08 Getting files to clients safely

IN ONE LINE

Unencrypted email attachments remain the default at most firms, and this is the easiest item on the list to fix properly.

Clients notice this one. A secure exchange method is among the few technology decisions that is visible to them, and handled well it reads as competence rather than friction — particularly for corporate and institutional clients who already work this way.

What to check

- [ ] A secure portal or encrypted exchange exists for anything sensitive.
- [ ] Clients are told at intake which channel to use, so the habit starts correctly.
- [ ] Large document sets do not travel by email.
- [ ] There is a defensible record of what was sent, to whom, and when.
- [ ] The method is simple enough that clients use it rather than replying with an attachment.

RED FLAG

A secure portal exists, but staff bypass it because it is slow or confusing. An unused control provides no protection and creates a false sense of one.

SCORE IT

Is there a secure client exchange method that staff and clients genuinely use?

☐ **0** no ☐ **1** exists but bypassed ☐ **2** in consistent use

09 Working outside the office

IN ONE LINE

The Law Society has published specifically on protecting client confidentiality while working remotely — treat every home office as part of the firm's footprint.

Remote work stopped being an exception some time ago, but the controls around it often never caught up with the practice. The awkward questions are usually physical rather than technical: who else can see the screen, and where do the printed pages end up.

What to check

- [ ] Remote access does not mean exposing a server directly to the internet.
- [ ] Nobody shares a set of remote access credentials.
- [ ] Printing at home has a rule, including how pages are disposed of.
- [ ] Video meetings use unique links; credentials are never reused or posted anywhere.
- [ ] There is guidance on public Wi-Fi, and on working in shared or family spaces.
- [ ] Firm data does not accumulate on personal machines as the path of least resistance.

THE HABIT THAT WORKS

One page of plain-language remote work guidance, issued once and re-sent when someone joins. It does not need to be a policy manual — it needs to be short enough that people finish reading it.

SCORE IT

Is there a written remote work standard covering access, printing and disposal?

☐ **0** no ☐ **1** verbal norms ☐ **2** written and communicated

10 Your domain, website and certificates

IN ONE LINE

Your domain name is the root of trust for your firm's email and identity — and a surprising number of firms don't fully control their own.

The domain is the quiet foundation under section 04. The same domain carries your email authentication, your website and your professional identity, and when a marketing agency or a long-departed contractor registered it, the firm is one lapsed renewal or one unreachable contact away from a genuine problem. This is unglamorous and rarely thought about until it fails publicly.

What to check

- [ ] The firm — not an agency, not an individual's personal account — is the registered owner of its domain, and can prove it.
- [ ] The registrar account has its own strong login and MFA, and someone current knows how to access it.
- [ ] Auto-renewal is on for the domain, and the billing card on file is not expired.
- [ ] TLS/SSL certificates for the website and any client portal renew automatically, and someone is alerted before they expire.
- [ ] DNS records are documented, and changes go through a known person rather than whoever set it up years ago.
- [ ] The website itself is patched and maintained if it runs on a content platform — an outdated plugin on the firm site is a public front door.

RED FLAG

Nobody at the firm can log in to the domain registrar, or the domain is registered under a former web designer's account. If the renewal notice goes to an inbox no one watches, the first sign of trouble is the website and email going dark together.

SCORE IT

Does the firm verifiably own its domain and DNS, with MFA on the registrar and automatically renewing certificates?

☐ **0** no or unsure ☐ **1** partially ☐ **2** yes, verified

11 Vetting a cloud provider and your vendors

IN ONE LINE

The Law Society of Alberta's cloud computing guidance directs lawyers to due diligence material prepared by the Law Society of British Columbia — there is no Alberta-specific checklist, so the diligence falls to you.

In practice this is less daunting than it sounds. Diligence here mostly means asking a provider a short list of direct questions and keeping the answers in writing. A provider who answers them readily is telling you something; so is one who does not. The same discipline applies to every outside party with a key to your systems, not only the headline cloud vendor.

Ask your provider, in writing

- [ ] Where is our data physically stored, and is any of it held outside Canada?
- [ ] Who at your organisation can access it, under what circumstances, and how is that access logged?
- [ ] If we leave, what do we get back — in what format, on what timeline, at what cost?
- [ ] If the Law Society requires records held in your systems, how quickly can they be produced?
- [ ] What is your breach notification commitment, stated in hours?
- [ ] What cyber liability insurance do you carry?
- [ ] Which subcontractors and subprocessors touch our data?
- [ ] The same questions get asked of every vendor with access to client data — not just the cloud provider, but the bookkeeper, the transcription service, the process server, and any marketing or web agency with access to your systems.
- [ ] You keep a simple list of who has access to what, and it is reviewed when a vendor relationship ends.

WORTH CONFIRMING

Alberta has its own private-sector privacy legislation alongside the federal regime, and cross-border or cross-provincial storage can engage both. Where a client relationship or a contract turns on this, confirm the position with counsel rather than with a vendor's marketing material.

SCORE IT

Do you have written answers from every provider and vendor with access to client data?

☐ **0** none ☐ **1** the main provider only ☐ **2** all, on file

12 Backup, continuity and succession

IN ONE LINE

The Law Society publishes a business continuity and succession planning guide and checklist — and most of what it asks for has a technology dependency underneath it.

Continuity planning tends to be treated as a document to be produced rather than a capability to be tested. The distinction becomes obvious at exactly the wrong moment. The single most valuable thing on this page is the test restore: a backup that has never been restored is a claim, not a safeguard.

What to check

- [ ] Backups exist, are held off-site, and cover every system on your data map — including Microsoft 365 and the practice management system, which are not automatically backed up just because they are in the cloud.
- [ ] A restore has actually been performed and documented within the last twelve months.
- [ ] Backups are protected against deletion by someone holding administrative credentials.
- [ ] At least one other person can reach critical systems if the responsible lawyer cannot.
- [ ] Administrative and recovery credentials live in a password manager the firm controls — not in one person's memory or a notebook in a drawer.
- [ ] You know, roughly, how long a full recovery would take, and that number is acceptable to the partners.

RED FLAG

Nobody at the firm has ever restored a file from backup. This is the most common finding on this page and the one with the widest gap between assumed and actual safety.

SCORE IT

Do backups cover every system and resist deletion, with a documented test restore in the last twelve months?

☐ **0** no ☐ **1** partially ☐ **2** yes, with a record

13 AI in the practice

IN ONE LINE

The risk is rarely the technology itself — it is privileged material being pasted into a consumer account whose terms you have never read.

Firms tend to arrive at one of two unhelpful positions: a blanket prohibition that staff quietly ignore, or no position at all. Neither is a policy. The workable middle is to decide what may be used, provide accounts on terms the firm has actually reviewed, and be explicit about what must never leave the firm's control.

What to check

- [ ] A written position on what may and may not be entered into an AI tool.
- [ ] Firm-provisioned accounts with reviewed data handling terms, rather than personal logins.
- [ ] An understanding of which tools you already pay for have AI features enabled by default.
- [ ] A named person responsible for verifying any output that reaches a client or a court.
- [ ] Consideration of client consent and confidentiality before AI touches matter content.
- [ ] The policy is short enough that people read it and specific enough to follow.

WORTH CONFIRMING

Professional obligations around competence, confidentiality and supervision apply to work assisted by these tools exactly as they do to any other work. Where a firm is setting policy, start from the Law Society's Generative AI Playbook and its model Gen AI use policy, and adapt rather than draft from scratch.

SCORE IT

Is there a written AI use policy, with firm-provisioned tools on reviewed terms?

- [ ] **0** neither
- [ ] **1** one of the two
- [ ] **2** both in place

14 What good IT support looks like

IN ONE LINE

Most firms discover what their IT provider is really worth during an incident — which is precisely when it is too late to renegotiate the terms.

These are the things worth agreeing in advance, in writing. They are also a fair way to assess an existing arrangement without changing anything: if a provider cannot produce documentation of your own environment on request, that is a finding in itself.

What to check

- [ ] Response times are defined in writing and vary by severity.
- [ ] You have a named contact who knows your firm, not only a shared queue.
- [ ] Documentation of your environment exists, is current, and belongs to you.
- [ ] You receive regular reporting you can understand — patching status, backup results, security alerts.
- [ ] After an incident, you get a written account of what happened, what was affected, and what changed as a result.
- [ ] Your provider brings you recommendations proactively rather than closing tickets and waiting.

RED FLAG

Following a security incident, your provider cannot tell you what occurred, which accounts were involved, or whether client data was accessed — and produces no written report. An incident you cannot explain is one you cannot demonstrate you handled.

SCORE IT

Is your support arrangement defined in writing — response times, documentation you own, regular reporting and incident follow-up?

☐ **0** no ☐ **1** partially ☐ **2** yes, all in writing

15 Cyber insurance and the controls behind it

IN ONE LINE

Every Alberta lawyer in private practice already carries base cyber coverage through ALIA — what varies is whether anyone knows what it covers, whether the limits fit the firm, and whether the controls attested to on any commercial policy are real.

Since the end of 2022, universal cyber coverage has been part of ALIA's mandatory indemnity program — so the question is not whether the firm is covered, but whether anyone knows how to invoke it. Beyond that base layer, commercial underwriting is a technical questionnaire whose answers are binding: carriers have declined claims when a forensic review found the attested controls were not in place on the day of the loss. Almost every section here matters twice — once for your clients, once for your coverage.

What to check

- [ ] You know where the firm's ALIA cyber coverage certificate is — the Lawyer Portal — what the coverage does, and how to report a claim, before you need to.
- [ ] Someone has assessed whether the base limits fit the firm's size and exposure, and whether excess or commercial coverage is warranted.
- [ ] The controls attested to on any application are genuinely in place — MFA enforcement, endpoint protection, backups, patching — and you could show evidence, not just say "yes."
- [ ] Someone reconciles the application answers against reality at each renewal, rather than copying last year's form.
- [ ] A written incident response plan exists, names who to call, and has been walked through at least once.
- [ ] The firm understands its own breach-notification duty under Alberta's Personal Information Protection Act — not only whether a provider would tell you, but what you must report, and to whom.

THE HABIT THAT WORKS

Treat any commercial application as a free annual audit: every "no" on the form is a gap worth closing before renewal, not a box to fudge.

SCORE IT

Do you know your ALIA cyber coverage, with attested controls evidenced and a written, tested incident response plan?

☐ **0** no ☐ **1** partially ☐ **2** yes, verified and evidenced

THE SCORECARD

Fifteen questions, one number.

Score each item 0, 1 or 2 using the guidance at the end of each section. The total is out of 30. The point is not the score itself — it is which items came back as zeros.

	QUESTION	0	1	2
01	IT owned by a named person, with budget and annual review	☐	☐	☐
02	Current written map of client data and access	☐	☐	☐
03	MFA enforced, legacy blocked, sign-ins monitored, same-day offboarding	☐	☐	☐
04	Email authentication, payment callback rule, awareness training	☐	☐	☐
05	Devices encrypted, managed, patched, disposal recorded	☐	☐	☐
06	Firewall supported, web filtering on, guest Wi-Fi separated	☐	☐	☐
07	Documents and email organised, retained and retrievable	☐	☐	☐
08	Secure client exchange method in consistent use	☐	☐	☐
09	Written remote work standard: access, printing, disposal	☐	☐	☐
10	Domain and DNS owned, registrar MFA, certificates auto-renew	☐	☐	☐
11	Written diligence answers on file from every vendor	☐	☐	☐
12	Backups cover all systems, deletion-proof, restore tested	☐	☐	☐
13	Written AI use policy with firm-provisioned tools	☐	☐	☐
14	Support in writing: response times, reporting, follow-up	☐	☐	☐
15	Cyber coverage known, controls evidenced, response plan tested	☐	☐	☐
	Total out of 30			_____

0–14

Material gaps that would be difficult to explain after an incident — or to an insurer. Start with items scored zero in sections 03, 04, 11 and 15.

15–22

A reasonable foundation with specific weak points. The fixes are usually small and the sequencing matters more than the spend.

23–30

Strong. Focus shifts to evidence and review cadence — being able to demonstrate the position, not only hold it.

A low score is not unusual and is not a judgement on the firm. Almost every practice we review scores zero on at least one item, and the most common is section 12. Knowing which one is the entire value of the exercise.

SOURCES AND FURTHER READING

Everything above, from the source.

Where this self-assessment refers to Law Society, ALIA or privacy material, here is the material itself — published by the source, free to access.

LAW SOCIETY OF ALBERTA

The Basics of Cloud Computing

Referenced in sections 01 and 11. Includes the two LSBC documents the Law Society of Alberta points lawyers to.

lawsociety.ab.ca → Resource Centre → Practice Management → The Basics of Cloud Computing

Protecting Client Confidentiality and Data Security While Working Remotely

lawsociety.ab.ca → Practice Management → Protecting Client Confidentiality… While Working Remotely

Business Continuity and Succession Plan Guide and Checklist

Referenced in section 12. A printable full version and templates are available on the same page.

lawsociety.ab.ca → Practice Management → Business Continuity and Succession Plan Guide and Checklist

Considerations for Choosing Accounting and Practice Management Software

Referenced in section 07. Includes an editable checklist.

lawsociety.ab.ca → Practice Management → Considerations for Choosing Accounting… Software

Annual Reporting — Trust Safety Accounting Upload

Referenced in section 07. Where the current list of approved accounting software vendors is maintained.

lawsociety.ab.ca → Trust Accounting and Safety → Annual Reporting

Practice and Equity Advisors

A free and confidential service for Alberta lawyers, articling students and legal support staff.

lawsociety.ab.ca → Lawyers and Students → Practice and Equity Advisors

The Generative AI Playbook

Referenced in section 13. Includes a model use policy firms can adapt.

lawsociety.ab.ca → Professional Conduct → The Generative AI Playbook

LAW SOCIETY OF BRITISH COLUMBIA

Cloud computing due diligence guidelines

Referenced in section 11. One of the two documents the Law Society of Alberta directs Alberta lawyers to.

lawsociety.bc.ca → Practice Resources → Cloud Computing Due Diligence Guidelines (PDF)

ALIA AND PRIVACY

Universal Cyber Coverage Program — ALIA (certificates and claims: Lawyer Portal) · Section 15

alia.ca/for-lawyers/cyber-coverage-program/

OIPC of Alberta — PIPA breach reporting · Section 15

oipc.ab.ca

Paths are current as of publication; if one no longer resolves, search the published title on the source site. Nothing here should be read as a statement of your professional obligations — the source documents govern.

WHO WROTE THIS

An Alberta IT firm, writing about Alberta firms.

AltaCom is a Calgary-based managed IT and cybersecurity company with a local Alberta team, supporting businesses across the province through managed services, project work and federal digital-adoption programs since 2011. Everything here comes from reviews we have run — the same fifteen questions, asked in real offices.

2011

Serving Alberta businesses since

Microsoft

Partner — Microsoft 365 and Azure

CDAP Advisor

Approved digital advisor under the Government of Canada's Canada Digital Adoption Program, 2022–2024

WHAT CLIENTS TELL US

> "AltaCom's team is exceptionally responsive, knowledgeable, and proactive. More importantly, they're a true partner to our firm. They don't just solve problems when they arise — they actively help us identify and implement technologies that improve efficiency, streamline operations, and create real value."
>
> Chetan Shory · Partner, Shory Law LLP · Google review

> "Incredible support and service. The team went over and above to help me solve the issues I had, but also talk through and understand the problem and how to avoid it in future."
>
> Emma Lindsey · Google review

AltaCom
An Abatri Solutions Inc. Company

NEXT STEP

We will do this with you, once, at no cost.

If you would rather not run through the fifteen sections alone, we will do it with you — a structured review of your environment against this scorecard. You leave with The Alberta Law Firm IT Guide — what to fix and in what order, written against your own scores. No obligation to change providers, and the guide is yours to keep either way.

It takes about thirty minutes. Most of that is us listening.

---

01 · Book

Scan the code or call. Thirty minutes, at your office or on a call.

02 · Review

We walk the fifteen sections with you and look at the systems behind them.

03 · Your guide

The IT Guide for your firm: findings, priorities, and what each fix takes.

SCAN TO BOOK

TALK TO US
403-744-5411

EMAIL
info@altacom.ca

BOOK ONLINE
altacom.ca/contact