IPMahir × CapabilityNext

Client data: standard operating procedures for independent finance professionals

What to do, step by step, in every situation that can put client information at risk: fifteen data-incident procedures, seven anti-money-laundering procedures, six routines, and the templates that go with them.

VERSION 1.0 · FOR REVIEW

Protect | Build | Prove | Grow

Issued by IPMahir with CapabilityNext · ipmahir.com · capabilitynext.com
November 2026 · For independent insurance, mortgage, investment and advisory professionals in British Columbia
A working procedure, not legal advice. Notification decisions are confirmed with your agency or dealer and your advocate.

HOW TO USE THIS DOCUMENT

One procedure for each situation, the same shape every time.

Print it, keep it where you work, and give a copy to every helper. When something goes wrong, find the matching procedure and work down the phases. Do not wait to understand everything before you start: the first fifteen minutes are always about stopping the exposure.

Part A · Incidents and money laundering

Twenty-two procedures. A1, fifteen data incidents: lost device, wrong recipient, phished account, SIM swap, fake instruction, malware and ransomware, vendor breach, leavers and shared logins, access requests, helper mistakes, AI tools, open links, paper records, device disposal. A2, seven anti-money-laundering procedures: identification, suspicious activity, large cash, politically exposed persons, third-party payers, the compliance programme and regulator requests.

Part B · Routines

Weekly, monthly, quarterly and annual checks, plus the checklists before adopting new software or taking on a helper. Routines stop most incidents.

Part C · Tools

Severity levels, the notification decision tree, a plain-words client notice, an incident log, a contact sheet and the evidence-file index.

Five rules that apply to every procedure

1	**Contain first.** Stop the exposure before you investigate. Change passwords from a clean device, not the one you suspect.
2	**Assume the worst until shown otherwise.** Stolen passwords usually mean stolen session tokens; ransomware usually means copied data.
3	**Tell people early, in plain words.** Clients should hear it from you. A prompt, honest message is judged far more kindly than a late one.
4	**Write it down as you go.** Dates, times, what you saw and what you did. The log is your evidence of reasonable care.
5	**Fix the cause, then close the log.** Each procedure ends with the change that stops it happening again.

Who does what

The professional

Owns the incident, makes the decisions in the decision tree, tells clients and the agency, and signs off the log. In a small practice this is you.

Helpers and family members

Report anything unusual the same day, without fear of blame. Never try to fix it alone or hide it.

Agency, dealer or compliance contact

Receives the same-day report and tells you what your agency requires. Their policy can be stricter than this one.

IPMahir

Supports containment, clean rebuilds, evidence collection and the fix. Call at the first sign of trouble; do not wait for the log.

Severity levels

Level	Meaning	What to do
High	Sensitive information (health, ID, bank, SIN or sign-in details) may be in the hands of an unauthorised person, or money is at risk.	Start now. Tell your agency the same day. Run the decision tree.
Medium	Client information was exposed to someone who may be trusted, or the data is less sensitive, or protection (such as encryption) reduces the risk.	Complete the procedure within 72 hours. Log it.
Low	Near miss: no client information left your control.	Log it and fix the cause. Near misses are free lessons.

PART A

Incident procedures

Each procedure lists a trigger, a severity guide, the owner, actions by phase, who to tell, what to record and the control it maps to in ISO/IEC 27002. The standard is the usual yardstick for "reasonable security"; following it is evidence of care, not a legal certificate.

SOP-01 Lost or stolen device (laptop, phone, tablet, USB stick)

TRIGGER	SEVERITY	OWNER
A device that holds, or can sign in to, client information is lost, stolen or missing for more than an hour.	High if unlocked, unencrypted or signed in. Medium if encrypted and locked.	The professional. Helper reports at once.

First 15 minutes	• Do not wait to see if it turns up. • Lock it from another device, then wipe it remotely if it cannot be recovered. • From a clean device, change your email and cloud passwords, sign out all sessions and revoke app access. • For a phone, call the carrier to suspend the SIM.
First hour	• Open your client-and-device map: which clients were on it (files, email, downloads, photos, chats, saved passwords)? • Check whether it was encrypted and screen-locked. That sets the level of harm. • If stolen, report to police and keep the file number.
Same day	• Use the notification decision tree (Part C) to decide who must be told. • Tell your agency or dealer compliance contact. • Tell affected clients where identity, bank or health details could be misused. • Open an entry in the incident log.
Within 72 hours	• Watch sign-in alerts and bank activity for affected clients. • Give clients plain advice on what to watch for. • Replace the device from a clean restore, not from a copy of the lost one.

Within 30 days	• Review why it was exposed: encryption, auto-lock, remote wipe, local copies, backups. • Fix the cause and note it in the log.

TELL AND RECORD
Agency or dealer; affected clients if harm is possible; police if stolen; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
8.1 User endpoint devices · 8.24 Use of cryptography · 5.9 Inventory of information and assets · 7.9 Security of assets off-premises · 8.13 Information backup
IPMahir: Device protection set-up, client-and-device map, first-hour call, evidence file entry.

SOP-02 Information sent to the wrong person (email, text, chat or shared link)

TRIGGER
Client information goes to someone who should not have it.

SEVERITY
High if health, ID or bank details. Medium otherwise.

OWNER
The sender.

First 15 minutes	• Try to recall the message. • Do not forward it, and do not open the attachment again. • If it was a shared link, switch the link off now. • Write to the recipient: it was sent in error, please delete it and confirm in writing.
First hour	• Save the sent item and your request as evidence. • List exactly what was sent (message, attachments, links). • Work out who the recipient is: another client, a known party or a stranger.
Same day	• Tell the client concerned, in plain words: what, when, what you did, what to watch for. • Tell your agency privacy contact. • Run the decision tree (Part C). Log the incident.
Within 72 hours	• Get the recipient's written confirmation of deletion. Follow up once if needed.
Within 30 days	• Turn off address auto-fill, switch on delayed send and external-recipient warnings. • Send documents by secure link, not attachment. • Add a recipient check to your training.

TELL AND RECORD
The client; agency privacy contact; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.14 Information transfer · 8.12 Data leakage prevention · 6.3 Awareness, education and training
IPMahir: Email settings review, secure document exchange, short training with this scenario as the example.

SOP-03 Phished sign-in or taken-over account (email, cloud, software, portal)

TRIGGER
You entered a password on a fake page, a login alert you did not cause, messages you did not write, or clients report odd messages from you.

SEVERITY
High. Treat as a breach until proven otherwise.

OWNER
The professional.

First 15 minutes	• From a clean device, change the password and sign out all sessions. • Revoke app access and tokens. Turn on authenticator-app sign-in. • Check forwarding rules, filters, delegates and recovery email or phone.

First hour	• Review login history, sent and deleted items. • List what the mailbox or system could reveal. • Warn contacts who received fake messages. • Change any other account that used the same password. Tell the software vendor.
Same day	• Decide harm: which clients' information could the attacker read? • Tell clients who received messages from your account. • Tell your agency. Run the decision tree. Log the incident. • If money moved or was requested, call your bank now and go to SOP-05.
Within 72 hours	• Scan the device for malware (SOP-06). Password theft often means the device is infected. • Monitor sign-in alerts.
Within 30 days	• Move all accounts to app-based or key-based sign-in. • Use a password manager. • Run a short scam-spotting session for everyone.

TELL AND RECORD

Contacts who got fake messages; affected clients; agency; software vendor; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT

8.5 Secure authentication · 5.17 Authentication information · 5.16 Identity management · 8.15 Logging · 8.16 Monitoring activities

IPMahir: Account hardening, sign-in alerts, access log review, scam-spotting session.

SOP-04 SIM swap or phone-number hijack

TRIGGER

Your phone suddenly has no signal, unexpected reset messages arrive, or clients mention messages you did not send.

SEVERITY

High.

OWNER

The professional.

First 15 minutes	• From another phone, call your carrier, report a SIM swap and get your number back. • From a clean device, secure email first (password, sign out all sessions), then cloud, software and bank accounts. • Switch from text-message codes to an authenticator app or key.
First hour	• Review recent sign-ins and transfers. • Contact your bank and card issuers. • Check your carrier account for changes.
Same day	• Warn clients and your agency about messages that came from you. • Decide harm and run the decision tree (Part C). Log the incident.
Within 72 hours	• Set a carrier PIN or number lock. • Remove phone-number recovery wherever you can.
Within 30 days	• Store your account recovery plan offline. • Rehearse it once.

TELL AND RECORD

Carrier; bank; clients who got messages; agency; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT

8.5 Secure authentication · 5.17 Authentication information · 5.15 Access control

IPMahir: Sign-in set-up that does not depend on text messages, recovery plan, rehearsal.

SOP-05 Fake instruction for money, bank details or documents

TRIGGER	SEVERITY	OWNER
A message that looks like a client, colleague or supplier asks you to move money, change bank details or send documents, and something feels wrong, or you already acted.	High if money has moved.	The professional.

First 15 minutes	• If you have NOT acted: stop. Do not reply. Phone the real client on the number you already hold. • If you HAVE acted: call your bank at once and ask for a recall; they can contact the receiving bank. • Do not use contact details from the message.
First hour	• Keep the original emails with headers. • Report to the police and the Canadian Anti-Fraud Centre (antifraudcentre-centreantifraude.ca). • Secure the mailbox (SOP-03): the sender may be inside your client's or your account.
Same day	• Tell the client by phone. • Tell your agency or dealer and your professional liability insurer, as their terms require. • Run the decision tree. Log the incident.
Within 72 hours	• Follow up with the bank and keep a record of every call.
Within 30 days	• Make the call-back rule permanent for every money or bank-detail instruction. • Require a signed form for bank changes. • Add a second approval above a set amount.

TELL AND RECORD	PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
Your bank; client; agency or dealer; insurer; police and fraud centre; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.	5.14 Information transfer · 6.3 Awareness, education and training · 8.5 Secure authentication **IPMahir:** Call-back procedure, signed-form template, scam-spotting training.

SOP-06 Malware, ransomware or password-stealing malware (including after a family download)

TRIGGER	SEVERITY	OWNER
Files are locked, a ransom note appears, antivirus alerts, odd emails go out from you, or a child or guest installed a game mod, cracked tool or "free upgrade" on a device that also touches work.	High. Assume saved passwords and sign-in tokens are stolen, and that data may have been copied.	The professional with IPMahir or your IT support.

First 15 minutes	• Disconnect the device from Wi-Fi and the network. Do not restart or wipe yet. Do not pay or negotiate. • From a clean device, change passwords and sign out all sessions. • Disconnect backup drives.
First hour	• Note the time and the ransom text. Photograph the screen. • List what the device could reach: email, cloud, software, client files. • Check that your backups are intact and not connected.
Same day	• Treat as a breach unless shown otherwise: ransomware often copies data before locking it. • Tell your agency and your insurer. Report to police and the fraud centre. • Run the decision tree. Log the incident.

Within 72 hours	• Rebuild from a clean image, not from the infected machine. • Restore from a tested backup. Rotate every credential. Confirm two-step sign-in.
Within 30 days	• Separate work and family devices. Allow installs only from official app stores. • Keep an offline backup and patch on a schedule.

TELL AND RECORD
Agency; insurer; police and fraud centre; clients if data was copied; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
8.7 Protection against malware · 8.13 Information backup · 8.19 Installation of software · 8.8 Management of technical vulnerabilities
IPMahir: Incident response, clean rebuild, backup design, work and family separation.

SOP-07 Notice that your software vendor has been breached

TRIGGER	SEVERITY	OWNER
A message from a vendor (or news) says client data in a system you use may have been accessed.	Medium to High, depending on what was accessed.	The professional.

First 15 minutes	• Check the notice is genuine: type the vendor's address yourself, do not click links in the email. Scammers copy these notices. • Change your password and turn on two-step sign-in. Sign out all sessions.
First hour	• Read what the vendor says was accessed, and when. • List which of your clients are in that system. • Write to the vendor: data categories, dates, steps taken, whether regulators were told, support offered.
Same day	• You remain responsible for client information your provider holds. Decide with your agency and advocate how and when to tell clients. • Run the decision tree. Log the incident.
Within 72 hours	• Send clients a clear notice if harm is possible. Follow vendor updates. • Check your connected apps.
Within 30 days	• Review the vendor: contract, security report, where data is stored. Decide whether to stay. • Update the vendor file.

TELL AND RECORD
Agency; affected clients; vendor; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.19 Information security in supplier relationships · 5.20 Security within supplier agreements · 5.22 Monitoring of supplier services · 5.23 Cloud services
IPMahir: Vendor due-diligence file, breach plan that includes "the vendor was breached".

SOP-08 Someone leaves, or a login is shared (leaver and access routine)

TRIGGER	SEVERITY	OWNER
A helper, assistant or locum leaves, you find a shared login, or it is time for the quarterly review.	Medium. High if a former person is still signing in.	The professional.

First 15 minutes	• On the day they leave, list every system they used. • Disable their individual logins. Change any shared password, then stop sharing it. • Revoke tokens and connected apps. Collect devices.

First hour	• Remove them from email forwarding, delegation, shared folders and calendars.
Same day	• Check the access log for the last 30 days: any downloads of client data? • Remind them in writing of their confidentiality duty.
Within 72 hours	• If a former person is still signing in, treat it as an incident: SOP-03 steps, log review and the decision tree.
Within 30 days	• Quarterly: export the user list of each system. Remove dormant accounts and unneeded rights. Confirm two-step sign-in for each account.

TELL AND RECORD
Agency if client data was accessed; affected clients if misused. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
6.5 Responsibilities after termination · 5.18 Access rights · 5.16 Identity management · 5.15 Access control
IPMahir: Leaver checklist, individual logins, quarterly access review calendar.

SOP-09 Client asks what information you hold about them (access request)

TRIGGER
A client, or someone on their behalf, asks for a copy of their information or asks you to correct it.

SEVERITY
Medium. The time limit is the risk.

OWNER
The professional.

First 15 minutes	• Write down the date you received it. • Acknowledge it in writing.
First hour	• Confirm who is asking: call back on a number you hold. If someone is asking for the client, confirm their authority in writing.
Same day	• Search every place: paper, email, each software system, phone, notes and backups. List what exists. • Mark information about other people, and anything you may withhold, and note the reason.
Within 72 hours	• Prepare the reply. Explain anything withheld, with reasons. Record a correction request if the client asks for one.
Within 30 days	• Reply in writing within the legal time limit (generally 30 days). Keep a copy of the request and your reply. • Check which vendors also hold the data.

TELL AND RECORD
The client; your agency privacy contact for anything you are unsure about. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.34 Privacy and protection of PII · 5.33 Protection of records
IPMahir: Client-data map, request log and reply template; training with a worked example.

SOP-10 A helper or colleague mishandles client information

TRIGGER
For example: a client's details read aloud in public, a screen photographed, a file sent to the wrong person, a login shared.

SEVERITY
Medium. High if sensitive details left your control.

OWNER
The professional.

First 15 minutes	• Stop the exposure: delete the photo or message, ask any recipient to delete it. • Stay calm. Learn the facts. Do not blame; people hide mistakes when they fear blame.
First hour	• List which clients and what details were involved.

Same day	• Tell affected clients if harm is possible. Tell your agency. • Run the decision tree. Log the incident.
Within 72 hours	• Give the helper short training on the specific habit. Record it.
Within 30 days	• Update the written rules and the day-one checklist for every helper. • Add the case, without names, to your training.

TELL AND RECORD
Affected clients if harm is possible; agency. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
6.3 Awareness, education and training · 6.8 Information security event reporting · 6.4 Disciplinary process
IPMahir: Helper training with a signed record, day-one checklist, incident form.

SOP-11 Client details pasted into a public AI tool

TRIGGER
Names, ID numbers, health or bank details were typed or uploaded into a chatbot, note taker or other public AI tool.

SEVERITY
Medium. High for health, ID or bank details.

OWNER
The person who used the tool.

First 15 minutes	• Stop. Take a screenshot of what was entered, with the time, tool and account. • Delete the chat and history. Use the tool's data controls to opt out of training and retention.
First hour	• Read the tool's terms: does it keep or train on what you type? Was it a work or personal account? • List which clients' details were entered.
Same day	• Assess sensitivity. Tell your agency. • Decide whether to tell the client: yes where health, ID or bank details were entered. • Run the decision tree. Log the incident.
Within 72 hours	• Ask the vendor for deletion if it offers it. Move the task to an approved tool.
Within 30 days	• Adopt an AI use rule: no real client details in public tools. • Add AI wording to client consent. Train everyone.

TELL AND RECORD
Agency; client where sensitive details were entered; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.10 Acceptable use of information and assets · 8.12 Data leakage prevention · 5.23 Cloud services
IPMahir: AI use rule, approved assistant, client wording, staff briefing.

SOP-12 The AI assistant or an automation sends something wrong

TRIGGER
An automated message goes to the wrong client, shows another client's details, or states something untrue.

SEVERITY
Medium. High if personal details were exposed.

OWNER
The professional who approved the assistant.

First 15 minutes	• Pause the assistant or automation so nothing more is sent.
First hour	• Find what was sent, to whom and what it showed. • Check the template, the data merge and the instructions.

Same day	• Correct in writing with each affected client, especially if advice or figures were wrong. • Tell your agency. Run the decision tree if personal information was exposed. Log the incident.
Within 72 hours	• Find the cause. Add an approval step and limits on what it can read and send. • Test with dummy data before switching it back on.
Within 30 days	• Review every automation and the activity log. • Update the AI use rule.

TELL AND RECORD
Affected clients; agency; regulator decision per Part C if personal information was exposed. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
8.15 Logging · 8.32 Change management · 5.10 Acceptable use
IPMahir: Approval steps, limits, activity log and a tested rollback for the connected assistant.

SOP-13 A shared link or folder is open to anyone

TRIGGER
A link set to "anyone with the link", a public folder, or a client mentions seeing their own document where they should not.

SEVERITY
Medium. High if sensitive documents were in it.

OWNER
The professional.

First 15 minutes	• Switch off the link or sharing now. • List the files that were reachable.
First hour	• Read the access or activity log: who opened or downloaded, and when.
Same day	• Tell affected clients if an unknown person accessed their documents. • Run the decision tree. Log the incident.
Within 72 hours	• Remove anything not needed from the folder.
Within 30 days	• Use named-person, expiring links from now on. • Audit all shared links every quarter.

TELL AND RECORD
Affected clients if accessed by an unknown person; agency; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.15 Access control · 8.3 Information access restriction · 5.12 Classification of information
IPMahir: Secure client upload portal, share audit and quarterly review.

SOP-14 Paper records lost, stolen or thrown away unshredded

TRIGGER
A file left in a car or cafe, a cabinet or office break-in, or papers discarded intact.

SEVERITY
High if ID copies, health or bank details.

OWNER
The professional.

First 15 minutes	• Secure the area. Report a theft or break-in to the police. • Use your file index to list what is missing.
First hour	• List the clients involved and the details on the papers. • Look for scanned or other copies.

Same day	• Tell affected clients if the papers could be misused. Tell your agency. • Run the decision tree. Log the incident.
Within 72 hours	• Monitor for misuse. Replace any records you must keep.
Within 30 days	• Lock cabinets. Keep paper out of cars and homes. • Scan and store securely. Use cross-cut shredding. Follow a retention schedule.

TELL AND RECORD
Police; affected clients; agency; regulator decision per Part C. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
7.1 Physical security perimeters · 7.7 Clear desk and clear screen · 7.14 Secure disposal or re-use of equipment
IPMahir: Records store, retention schedule, secure disposal routine.

SOP-15 Retiring, selling, recycling or replacing a device

TRIGGER
Any device that has held client information leaves your hands.

SEVERITY
Medium. A common and avoidable exposure.

OWNER
The professional.

First 15 minutes	• Confirm your backup is complete and tested.
First hour	• Sign out of every account. Remove the device from account device lists and "find my" services.
Same day	• Erase and reset the device, including encryption keys. Remove the SIM and memory cards.
Within 72 hours	• Record the make, serial number, date and method in your device list.
Within 30 days	• If recycling, use a certified recycler and keep the receipt.

TELL AND RECORD
No one, unless the reset was skipped: then treat as SOP-01. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
7.14 Secure disposal or re-use of equipment · 7.10 Storage media · 5.9 Inventory
IPMahir: Retirement checklist and device list.

PART A2

Anti-money-laundering and fraud-prevention procedures

Reporting duties under Canada's anti-money-laundering law differ by sector (life insurance, mortgage, securities and others) and by whether you are a reporting entity yourself or work under your agency, dealer or insurer. Confirm with your compliance contact and FINTRAC's guidance which duties apply to you. Timings below follow FINTRAC guidance and are marked for your advocate to confirm. These procedures also protect the identity records you must keep: use Part A when those records are lost or exposed.

SOP-16 Identify and verify a client, payer or third party

TRIGGER	SEVERITY	OWNER
A new client, a new payer, a change of owner or beneficiary, or any transaction where your sector requires identification. Do this before the transaction goes ahead.	Medium. A missed or weak check is a compliance failure and a fraud risk.	The professional who meets the client.

Before you start	• Ask your compliance contact which transactions in your sector require identification, and which methods are accepted. • Explain to the client why you need it. Your privacy notice should say so. • Prepare the record form so nothing is missed.
At the meeting	• Check the original document: valid, not expired, and the photo matches the person. • Record: full name, date of birth, address, occupation, document type, number, place of issue, expiry date, date checked and who checked it. • If someone else is paying or benefits, record who they are and their link to the client. For a company or trust, record who owns and controls it. • Never accept a photo of an ID sent by ordinary text or email.
Same day	• File the record in the protected identity-records store. Delete any temporary copies from phones, downloads and email. • Enter the check in the verification log.
If you cannot verify	• Do not proceed with the transaction. • Write down why you could not verify. Tell your compliance contact the same day. • If anything about the refusal looks suspicious, go to SOP-17.
Ongoing	• Keep records for the required period (generally five years). Keep them protected and retrievable. • Refresh information for higher-risk clients.

TELL AND RECORD

Compliance contact for any failed verification. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT

5.34 Privacy and protection of PII · 5.33 Protection of records · 8.3 Information access restriction · 7.14 Secure disposal

IPMahir: Protected identity-records store, record forms, retrieval test, training. The compliance officer role stays with you or your agency.

SOP-17 Suspicious activity or attempted transaction (suspicious transaction report)

TRIGGER	SEVERITY	OWNER
You have reasonable grounds to suspect that a transaction, or an attempted transaction, is related to money laundering or terrorist financing. See the red flags in Part C.	High. Time matters and secrecy matters.	The professional notices; the compliance officer reports.

In the moment	• Stay polite and calm. Ask the ordinary business questions you would normally ask. • Do not accuse the client or hint at suspicion. • Do not accept cash or process the transaction until you have spoken to your compliance contact. • Write down exactly what was said and done: who, when, amounts, documents, behaviour.
Same day	• Tell your compliance officer or agency compliance contact the same day, in person or by phone, not by casual message. • Keep the original documents and notes. Do not discuss it with colleagues who do not need to know.
As soon as practicable	• The compliance officer decides whether the grounds are met and files the suspicious transaction report with FINTRAC as soon as practicable after the grounds to suspect are established. • Keep a copy of the report and your notes, protected, with restricted access.
What you must not do	• Do not tell the client, or anyone who might tell them, that a report is being made or considered. Tipping off can be an offence. • Do not delete or alter records. Do not investigate by yourself.
Afterwards	• Agree with the compliance officer whether to continue or end the relationship. • Ask what control would have caught this earlier, and add it. • Store STR files separately with limited access.

TELL AND RECORD	PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
Compliance officer. FINTRAC via the compliance officer. Not the client. Record the date, time, what happened and what you did in the incident log.	5.33 Protection of records · 8.3 Information access restriction · 6.6 Confidentiality or non-disclosure agreements **IPMahir:** Escalation script, red-flag card, protected STR records store. IPMahir does not make the reporting decision.

SOP-18 Large cash received ($10,000 or more)

TRIGGER	SEVERITY	OWNER
You or your agency receive $10,000 or more in cash in one transaction, or in several cash amounts from or for the same person totalling $10,000 or more within 24 hours.	Medium. Reporting deadline applies.	The compliance officer, with the professional.

At the time	• Many agencies do not accept cash at all. If your agency does not, say so politely and decline. It is the strongest control. • If cash is accepted: identify the person handing it over (SOP-16) before accepting it, and record on whose behalf. • Count it with a witness and give a receipt.
Same day	• Record the transaction in the cash log. Deposit as your policy requires. • Ask yourself whether anything is suspicious. If yes, go to SOP-17 as well.
Within the deadline	• The compliance officer files a large cash transaction report with FINTRAC within the time limit (15 calendar days after the transaction).

If it looks like structuring	• Several amounts just under the threshold, spread over days or offices, is a warning sign. Treat it as SOP-17. Never explain to a client how to avoid a report.
Afterwards	• Keep a copy of the report, the cash log and the identification record for the required period.

TELL AND RECORD
Compliance officer; FINTRAC via the compliance officer. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.33 Protection of records · 5.34 Privacy and protection of PII
IPMahir: Cash log template, reporting calendar, protected records store.

SOP-19 Politically exposed person, head of an international organisation, or their family and close associates

TRIGGER
A new or existing client may hold, or have held, a prominent public position, or be a family member or close associate of such a person, or you are unsure.

SEVERITY
Medium to High. Needs enhanced care, not refusal by default.

OWNER
The professional with the compliance officer.

At onboarding	• Ask the question in plain words at onboarding. Check public information if the answer is unclear. • Remember that being a politically exposed person is not a crime.
Before you proceed	• If the answer is yes or likely, follow your agency policy before going ahead, which normally includes approval from senior management. • Establish the source of funds and the source of wealth and ask for supporting documents.
Same day	• Record the determination, who approved it and why. Add the client to your higher-risk list.
Ongoing	• Apply enhanced monitoring: review activity more often and look for changes in pattern. • Treat unusual activity under SOP-17.
Review	• Review yearly. Remove the flag only as the rules allow, and record why. • Confirm with your compliance contact exactly which requirements apply to your sector and products.

TELL AND RECORD
Compliance officer; senior management as your agency policy requires. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.34 Privacy and protection of PII · 5.33 Protection of records
IPMahir: Onboarding question script, higher-risk register, review calendar.

SOP-20 Third-party payer, unclear ownership or unexplained source of funds

TRIGGER
The person paying is not the client; money comes from a foreign or unrelated account; a large premium, deposit or down payment has no clear source; a company or trust client has unclear owners.

SEVERITY
Medium. High if the explanation does not fit the client.

OWNER
The professional.

At the meeting	• Ask who is paying and why, and where the money comes from, in plain words. • Write down the answers in the client's own terms.
Same day	• Verify the payer as you would a client (SOP-16). For companies and trusts, record the owners and controllers. • Compare the explanation with what you know about the client's means and business.

If it does not add up	• If the explanation is vague, changes, or does not fit, treat it as SOP-17 and tell the compliance officer. • Do not accept the funds until you have the compliance officer's view.
Afterwards	• File the explanation and the evidence with the client record.
Review	• Review third-party payments quarterly. Your policy may decline payments from unrelated third parties altogether.

TELL AND RECORD
Compliance officer. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.33 Protection of records · 5.34 Privacy and protection of PII
IPMahir: Source-of-funds question card, payer record, quarterly review checklist.

SOP-21 Compliance programme: set up and review

TRIGGER
You are a reporting entity or work under one: at start-up, every year, and at least every two years for the full effectiveness review.

SEVERITY
Routine. Gaps here are what examiners find.

OWNER
The compliance officer.

Set up	• Appoint a named compliance officer and a back-up. Record the appointment.
Written procedures	• Write down your policies and procedures: identification, record keeping, reporting, politically exposed persons, ongoing monitoring.
Risk assessment	• Assess your risk: clients, products and services, how you deal with clients, where they and their money are, and any new technology you use. Update it yearly.
Training	• Keep a written training plan and run training for everyone who deals with clients. Keep attendance records.
Review	• Review the effectiveness of the programme at least every two years, and report the findings to senior management. Keep the report. • Confirm with your compliance contact which of these apply to you directly and which are covered by your agency or insurer's programme.

TELL AND RECORD
Senior management or the agency principal. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT
5.1 Policies for information security · 5.36 Compliance with policies and standards · 6.3 Awareness, education and training
IPMahir: Procedure templates, risk assessment worksheet, training record, evidence file.

SOP-22 FINTRAC or another regulator asks for records, or an examination begins

TRIGGER
A letter, call or notice from FINTRAC, the Insurance Council, a dealer or an insurer asks for records or announces a review.

SEVERITY
High. Deadlines apply.

OWNER
The compliance officer and the professional.

First 15 minutes	• Do not ignore it, and do not delay. • Note the date and time. Read exactly what is asked and the deadline. • Check the contact is genuine by calling back on an official number. Scammers impersonate regulators.

First hour	• Tell your compliance officer, your agency and your advocate. • Stop routine deletion of any related record.
Same day	• Collect the records from your protected store. Give only what is asked, and no more. • Log what you collect and what you send.
Within the deadline	• Reply in writing and by a secure channel, within the deadline. • If you need more time, ask in writing before the deadline.
Afterwards	• Debrief. Fix any gap found and update the evidence file.

TELL AND RECORD

Compliance officer; agency; advocate. Record the date, time, what happened and what you did in the incident log.

PREVENTION (ISO 27002 CONTROLS) · IPMAHIR SUPPORT

5.33 Protection of records · 5.31 Legal, statutory, regulatory and contractual requirements · 8.15 Logging

IPMahir: Records retrieval, secure transfer and a rehearsal of this procedure.

PART B

Routines that stop most incidents

R1 · Weekly (15 minutes)

- Check sign-in alerts and unusual activity on email and each software system.
- Check that updates have installed on every device.
- Check mailbox forwarding rules and filters.
- Confirm last night's backup ran.

R2 · Monthly (30 minutes)

- Install any pending updates and restart devices.
- Review shared links and folders; switch off any not needed.
- Restore one file from backup to prove it works.
- Review the password manager for weak or reused passwords.

R3 · Quarterly (60 minutes)

- Run the access review for every system (SOP-08).
- Check the vendor list for changes or notices.
- Review the incident log for patterns.
- Hold a 15-minute refresher for everyone who handles client information.

R4 · Annually (half a day)

- Repeat the free health check and compare the ratings.
- Rehearse your breach plan, including "the vendor was breached".
- Review every policy and update the evidence file.
- Review client consent wording, including AI use.
- Review every vendor: contract, security report, storage location.

R5 · Before adopting any new software, app or AI tool

- What client data will it hold or read? Where is it stored?
- What does the contract say about breach notice and deletion?
- Can it use individual logins with two-step sign-in? Can you export and delete data?
- Which AI features are on by default? Switch off what you do not need.
- Is there an exit plan? Record the decision in the vendor file.

R6 · Before a new helper starts

- Training and signed rules before any access.
- Individual logins and the minimum access needed.
- Work devices only, protected as in the device list.
- Written confidentiality commitment; leaver steps agreed in advance.

PART C

Tools

C1 · Notification decision tree

> **Step 1. Contain.** Has the exposure been stopped (device wiped, link off, password changed, assistant paused)? If not, do that first.
>
> **Step 2. What was involved?** List the clients and the kinds of information: health, identity documents, SIN, bank or account numbers, sign-in details, or only contact details.
>
> **Step 3. Could it cause harm?** Could the information be used for fraud, identity theft, blackmail, discrimination or embarrassment? Was it protected (encrypted, locked), and who may have had it: a stranger, a known client, a trusted person? If harm is possible, treat as **High**.
>
> **Step 4. Tell your agency or dealer.** Same day, for any High or Medium incident, and sooner if their policy says so.
>
> **Step 5. Tell affected clients.** Promptly, in plain words, whenever harm is possible. Use template C2. When in doubt, tell.
>
> **Step 6. Regulators and others.** Decide with your agency and your advocate whether the privacy regulator, the Insurance Council or another regulator, your insurer, the police or the fraud centre should be told. Federal privacy law requires reporting by organisations it covers when there is a real risk of significant harm. BC's commissioner recommends that private organisations report breaches voluntarily. [Advocate to confirm which rules apply to each practice.]
>
> **Step 7. Record.** Enter every decision and the reason in the incident log, including a decision not to notify.

C2 · Plain-words notice to a client

Dear [name],

I am writing to tell you that on [date] [what happened, in one sentence]. The information involved was [kinds of information]. I do not know of any misuse so far. [Or: I have seen the following misuse: ...]

What I have done: [stopped the exposure; secured accounts; informed my agency; other steps].

What you can do: watch your bank and card accounts for anything unusual; change the passwords on your online accounts if you reused any; be careful with any message claiming to come from me or from your bank asking for details or money, and phone me on [number you already have] to check; contact your bank if you see anything unusual.

I am sorry this happened. If you have any questions, please call me on [number] or write to [email]. I will update you if I learn anything more.

[Name, role, agency]

C6 · Anti-money-laundering reports at a glance [advocate to confirm for each sector]

Report or duty	When	Who decides or files
Suspicious transaction report	As soon as practicable after reasonable grounds to suspect are established, including for attempted transactions. Never tell the client.	Compliance officer
Large cash transaction report	Within 15 calendar days of receiving $10,000 or more in cash, singly or within 24 hours.	Compliance officer
Terrorist property report	Immediately, when you know property belongs to or is controlled by a listed person or group.	Compliance officer, with the police as required
Identification records	Kept for the required period (generally five years), retrievable on request.	Professional and compliance officer

C7 · Red flags by sector

Sector	Warning signs
Insurance	Cash premiums, or premiums paid by a person unrelated to the policyholder; payment from several accounts or from abroad; early cancellation or surrender with a penalty and a request to pay out to a third party; overpayment followed by a refund request; policies far beyond the client's means; frequent changes of owner or beneficiary.
Mortgage	A large deposit or down payment with no clear source; gifted or third-party funds that do not fit; early payoff by a third party; rapid purchase and sale; private lenders or guarantors who cannot be explained; a client who avoids documents.
Investments	Deposits from third parties; money in and then straight out with little activity; several deposits just under a reporting limit; account details that do not match the client; instructions that change often; a client unwilling to say why they are investing.
Any sector	Reluctance to give ID or information; ID that looks altered; urgency with no reason; a client who asks how to avoid reports; an explanation that changes; transactions that make no business sense; pressure on you to skip checks; an offer of a reward to look away.

C3 · Incident log

No.	Date and time found	What happened	Clients and data	Actions and who was told	Cause and fix

C4 · Contact sheet (fill in and keep with this document)

Agency or dealer compliance contact	
Agency privacy contact	
Bank and card issuer fraud lines	
Phone carrier fraud line	
Professional liability and cyber insurer	
Your advocate	
IPMahir support	ipmahir.com
Software vendors (name, support line, account number)	

C5 · Evidence file index (one page)

Item	Where it is kept and date last reviewed
Device list and protection record	
Client-and-data map (where information sits)	
Access list per system and last review date	
Vendor file: contract points, storage location, security report	
Retention schedule and a retrieval test	
Breach plan, contact sheet and last rehearsal date	
Training record and signed helper rules	
AI use rule and client consent wording	
Incident log	

Sources. Insurance Council of BC guidance on client confidentiality and on generative AI; the BC privacy commissioner's guidance on protecting personal information away from the office and on breach notification; the Canadian Centre for Cyber Security baseline controls for small organisations; ISO/IEC 27002; FINTRAC guidance for reporting entities. IPMahir and CapabilityNext are independent of every regulator, insurer and dealer named here, and this document is not legal advice.

APPENDIX

Statutes, rules and standards these procedures support

Each procedure in this document supports the instruments below. We support and evidence compliance; we do not certify, audit as a regulator, give legal advice or guarantee compliance. Which instruments apply depends on your licence, products and employer, so confirm with your agency or dealer compliance contact and your advocate. Full detail and official sources: **capabilitynext.com/compliance-coverage**.

Statutes

Instrument	How these procedures and our services support it
Personal Information Protection Act (British Columbia) SBC 2003, c. 63	Privacy training for you and your helpers; technical safeguards and an evidence file; access-request and wrong-recipient procedures; vendor due-diligence file; client consent wording.
Personal Information Protection and Electronic Documents Act (PIPEDA) SC 2000, c. 5	Breach plan and notification decision tree; incident log; breach procedures SOP-01 to SOP-15.
Proceeds of Crime (Money Laundering) and Terrorist Financing Act and its regulations SC 2000, c. 17	Anti-money-laundering procedures SOP-16 to SOP-22; protected identity-records store and retrieval test; compliance-programme templates; training. The compliance officer role and every reporting decision stay with you or your agency.
Canada's Anti-Spam Legislation (CASL) SC 2010, c. 23	Consent records and opt-outs built into the connected assistant; outreach drafted for your approval before it is sent.
Financial Institutions Act (British Columbia), insurance licensing RSBC 1996, c. 141	Client-file, privacy and cyber safeguards that support the Council's expectations on confidentiality; training record; evidence file.
Mortgage Brokers Act (British Columbia) RSBC 1996, c. 313	Protected mortgage-file records, access reviews, closed-file clean-up and backups with an evidence file.
Securities Act (British Columbia) and the rules of the Canadian Investment Regulatory Organization RSBC 1996, c. 418	Secure exchange for know-your-client forms, call-back routine for instructions, protected records and a dealer-ready evidence file.

Regulators' rules and guidance

Source	How we support it
Insurance Council of British Columbia: rules and guidelines	Safeguards, training and an AI use rule that match the Council's published expectations.
BC Financial Services Authority: mortgage broker rules and guidance	Protected files, retention schedule and evidence file for mortgage practices.
Canadian Investment Regulatory Organization (CIRO): dealer and rep rules	Evidence file and procedures you can show your dealer on request.
FINTRAC guidance for reporting entities	SOP-16 to SOP-22, reporting calendar, red-flag cards and a protected records store.
BC Information and Privacy Commissioner: guidance	Home and device safeguards, breach procedures, AI use rule.
Joint principles for responsible generative AI from Canada's privacy regulators	Approved assistant, no client details in public AI tools, human check on anything sent to a client, consent wording.
Canadian Centre for Cyber Security: baseline controls for small and medium organisations	The device, account, backup and home-network safeguards in our implementation list.

ISO standards

Standard	How we use it
ISO/IEC 27002:2022 Information security controls	Every safeguard and every procedure is mapped to its control number, with a one-page evidence file.
ISO/IEC 27001:2022 Information security management systems	Our method follows the same cycle at small-practice scale. We do not certify; a certification body does.
ISO/IEC 27701 Privacy information management	Our privacy training, access-request procedure and retention schedule follow its structure.
ISO/IEC 27017 and ISO/IEC 27018 Cloud security and protection of personal information in public clouds	Vendor due-diligence file for each software system, and the cloud-only practice review.
ISO/IEC 42001:2023 Artificial intelligence management system	AI use rule, approval step, activity log and review calendar for the connected assistant.
ISO 31000 Risk management and ISO 22301 Business continuity	Health-check ratings, risk assessment worksheet, backup design and breach-plan rehearsal.