

Incident Response Plan Template

A fill-in plan for a small software company: who decides, how you judge severity, what to do in each phase, and who you have to tell, including under Canadian privacy law. Fill in the blanks, get it approved, then test it with a one-hour tabletop exercise.

Updated September 2026. Structure follows the common incident life cycle (prepare, detect and analyse, contain, eradicate and recover, learn), the same shape as NIST SP 800-61. Written so it satisfies what SOC 2, ISO 27001, cyber insurers and enterprise buyers ask to see.

1. Purpose and scope

This plan applies to any event that threatens the confidentiality, integrity or availability of _____ (company name) systems or the data we hold, including customer data and personal information.

Plan owner: _____ Approved by: _____ Date: _____

Reviewed at least every 12 months, and after every Severity 1 or 2 incident.

2. Roles

Small teams combine roles. What matters is that each role has a named person and a backup, and that everyone knows who has the final say.

Role	Responsibility	Primary	Backup
Incident lead	Declares the incident, sets severity, makes decisions, keeps the timeline.		
Technical lead	Investigates, contains, fixes, preserves evidence.		
Communications lead	Customer, staff and public messages; single voice outside the team.		
Privacy and legal	Decides on notification duties to regulators, individuals and customers.		
Executive sponsor	Approves spending, external help and public statements.		

Contacts you will need in a hurry

Who	Name and number
Cyber insurer claims line and policy number	
Breach coach or outside counsel	
Forensics or incident response firm (insurer panel, if required)	
Cloud provider support (plan level and case process)	
Domain registrar and DNS provider	
Police cybercrime unit, and the Canadian Anti-Fraud Centre for fraud	

Call your insurer early. Many cyber policies require notice within a set period and use of their panel vendors. Hiring your own forensics firm first can put coverage at risk. Check your policy now, not during an incident.

3. Severity levels

Level	Examples	Response
Sev 1	Confirmed access to customer data or personal information; ransomware; production down for all customers.	All roles engaged immediately, executive informed within 1 hour, insurer notified.
Sev 2	Suspected data access under investigation; compromised staff account with production access; major outage.	Incident lead and technical lead within 1 hour; review privacy duties within 24 hours.
Sev 3	Malware on one laptop, contained; phishing that captured a credential with no evidence of use.	Handled in working hours; logged.
Sev 4	Blocked attack, policy violation with no data exposure.	Logged and reviewed weekly.

When unsure, rate higher. It is easier to stand down than to catch up.

4. Response phases

Prepare (before anything happens)

- Logging is centralised and kept at least 12 months, so you can investigate after the fact.
- Admin access uses MFA, and there is a documented break-glass account.
- Backups are tested, and at least one copy cannot be changed or deleted by a compromised admin account.
- Staff know how to report something suspicious: _____ (channel).

Detect and analyse

- Open an incident record and start a timeline in UTC: what was seen, by whom, when.
- Set a severity level. Name the incident lead.
- Work out scope: which systems, which accounts, which data, since when.
- Preserve evidence before changing things: snapshots, log exports, copies of suspicious files. Record who handled each item.

Contain

- Short term: disable compromised accounts, revoke sessions and keys, isolate affected hosts, block attacker infrastructure.
- Rotate credentials the attacker may have seen, including API keys and CI secrets.
- Do not wipe systems before evidence is preserved unless the harm of waiting is greater.

Eradicate and recover

- Remove the cause: the vulnerable component, the malicious access, the persistence.
- Restore from known-good backups where needed and confirm integrity.
- Watch closely for return activity for at least two weeks.

Learn

- Hold a blameless review within 10 business days for Sev 1 and 2.
- Record the root cause, what worked, what did not, and actions with owners and dates.
- Update this plan, the risk register and any affected controls.

5. Who to notify, and when

The privacy and legal lead makes these decisions, with counsel for Sev 1 and 2. Record every decision and the reason, including a decision not to notify.

Who	When it applies	Timing
Office of the Privacy Commissioner of Canada and affected individuals (PIPEDA)	A breach of security safeguards involving personal information that creates a real risk of significant harm.	As soon as feasible. Keep a record of every breach, reportable or not, for 24 months.
Commission d'accès à l'information and affected individuals (Quebec Law 25)	A confidentiality incident involving Quebec residents' personal information that presents a risk of serious injury.	Promptly. Record every incident in your confidentiality incident register.
Alberta and British Columbia commissioners	Alberta PIPA requires notifying the Commissioner of incidents with a real risk of significant harm. Check provincial rules for where your customers and data are.	Without unreasonable delay.
Customers	Whatever your contracts and DPAs say. Many set 24 to 72 hours from confirmation.	Per contract: _____
US and EU authorities	US state breach laws and, for EU personal data, the GDPR (72 hours to the supervisory authority where required). HIPAA business associates notify the covered entity within 60 days at most.	Per law and contract.
Cyber insurer	Any incident that may lead to a claim.	Per policy: _____

First customer message: a template

Keep it factual. Say what you know, what you do not know yet, what you are doing, and when you will update them. Do not speculate about cause or blame.

Subject: Security incident affecting [service]

On [date] we identified [what happened, in one sentence]. We have [containment step taken]. Based on what we know now, [what data or service is affected, or "we are still determining whether your data is affected"]. We will update you by [time and date]. Your contact for this incident is [name, email, phone].

6. Testing this plan

Run a tabletop exercise at least once a year and when the team changes. One hour is enough. Suggested scenarios:

- A developer's laptop is stolen with an active session to your cloud console.
- A customer emails to say their data appeared on a paste site.
- Ransomware encrypts your shared drive on a Friday evening.
- A third-party vendor tells you they were breached and held your customer list.

Record the date, attendees, scenario, gaps found and actions. That record is the evidence auditors and insurers ask for.

Common mistakes

- A plan that names roles but not people, or names people who have left.
- No out-of-band channel. If your email or chat is compromised, how does the team talk?
- Wiping and rebuilding before evidence is saved, which makes it impossible to know what was taken.
- Deciding not to notify without writing down why.
- Never testing the plan until the real thing.

What to do next

1. Fill in every blank above this week, especially the insurer and contacts table.
2. Have the executive sponsor approve the plan, and tell staff how to report an incident.
3. Book a one-hour tabletop within 30 days and write down what you learn.
4. Check your customer contracts for notification periods and list them here.

Want a second pair of eyes? TrazTech runs security and compliance readiness as fixed-scope work for software companies. Book a free 30-minute readiness call at traztech.ca/free-readiness-call, or get The Compliance Brief, one short email every Tuesday, at traztech.ca/brief.