CYBERSECURITY STARTER KIT

# Getting Started

The kit guide: which documents, in what order and why. Plan a few hours, spread over a month.

A small business does not need a security department to be well prepared. It needs **clear rules for its employees**, a **plan to get back up and running**, **steps to follow when it happens** and **evidence to show its insurer**. That is exactly what this kit contains.

## What's in the kit

| No. | Document | Format | Filled in by |
|---|---|---|---|
| 1 | IT Acceptable Use Policy (to be signed by each employee) | Word | Management |
| 2 | IT Disaster Recovery Plan | Word | Management + IT |
| 3 | Cybersecurity Incident Response Plan | Word | Management + IT |
| 4 | Incident Report Form | Word | Employees |
| 5 | Asset and Vendor Inventory | Excel | IT |
| 6 | Privacy Incident Register (Quebec Law 25) | Excel | Privacy officer |
| 7 | Cyber Insurance Readiness | Excel | Management + IT |
| 8 | First Steps in Case of a Cyberattack (poster) | PDF | Print it |
| 9 | Emergency Contacts | Word | Management |

## The four-week plan

### Week 1 — Be ready to react (1 hour)

- ☐ Fill in sheet **9 – Emergency Contacts** and keep a copy outside the office.
- ☐ Print and post **8 – First Steps** near workstations.
- ☐ Name the person in charge of the protection of personal information and open **6 – Law 25 Register**.

### Week 2 — Set rules for employees (1 to 2 hours)

- ☐ Adapt **1 – Acceptable Use Policy**, present it to the team and have it signed.
- ☐ Hand out **4 – Incident Report Form** and explain that whoever reports is not blamed.

### Week 3 — Know what you protect (2 hours, with your IT provider)

- ☐ Fill in **5 – Inventory**: devices, software, suppliers, administrator accounts.

- ☐ Complete **2 – Disaster Recovery Plan**: priorities, acceptable delays, backups.

### Week 4 — Prepare for the worst and for the insurer (2 hours)

- ☐ Adapt **3 – Incident Response Plan** and run a 30-minute exercise: “an employee calls, their files are encrypted”.
- ☐ Fill in **7 – Cyber Insurance Readiness** and fix the missing critical controls first.

## The five protections every insurer checks

- **Multi-factor authentication (MFA)** on email, remote access and administrator accounts.
- **EDR** (next-generation antivirus with detection and response) on all computers and servers.
- **Immutable or offline backups**, tested at least once a year.
- **A payment procedure**: any banking change is confirmed by phone.
- **Employee training**, at least once a year.

If even one is missing, the premium goes up, an exclusion applies… or a claim may be denied.

## Learn more

Articles on our blog **supportadistance.com/en/blog-and-news**:

- 12 steps to protect your business: /en/12-steps-protect-business-2026/
- CEO fraud: /en/ceo-fraud/
- Payroll fraud: /en/payroll-diversion-fraud/
- Hacked account, 5 steps: /en/hacked-account-5-steps/
- Passkeys: /en/passkeys-microsoft-sms/

> **Need help filling in the kit?**
>
> Appelez le tech can assess your environment, fill in the inventory and the insurer checklist with you, and put the missing protections in place.
>
> **514-444-1041** · supportadistance.com/en/contact

*These documents are templates to adapt. They are not legal advice; review legal and contractual obligations with your legal advisor or insurance broker.*