Loss prevention: be proactive!

Protect your business against privacy breaches

FORMAL PROCEDURES HELP TO KEEP PERSONAL INFORMATION SAFE

Confidential data whether physical or digital, should be securely stored with access restricted to authorized individuals.

- Ensure access to computers or files require proper authorization (secure logins, rotating passwords, etc.).
- Keep shared office equipment like printers, fax and copy machines, as well as collection areas for mail, employee inboxes and processing bins for documents, in secure areas away from public access.
- Keep paper files containing personal data about customers, clients, patients, accounts or employees in locking cabinets, locked rooms, or other areas that allow for authorized access only.
- Put written procedures in place to define who may view, edit or delete personal information. Configure the computer network to make sure only these individuals have access to specific areas or files.
- Restrict access to confidential information to only those individuals who need it for their work. Make it inaccessible to people working outside of normal business hours as well as cleaning, maintenance and security staff.

Identify essential information to retain

To comply with the Personal Information Protection and Electronic Documents Act ("PIPEDA") and applicable provincial privacy legislation, you must ensure that this personal information is kept confidential and stored securely.

- Collect and store only the information that is critical for the business.
- Put a document retention policy in place.
- Make sure outdated information is destroyed in a secure manner

Put security systems in place

Install a burglar alarm system with perimeter and volumetric sensors connected to an approved monitoring station.

Require sign-in for non-employee visitors

Prior to being allowed inside your office, all visitors should show identification and sign in. This includes vendors, customers and job applicants.

03-M-181.1e (09-18)

Evaluate contractor or vendor access to information

Determine which services require access to confidential information and restrict access so that only the contractors or suppliers providing these services can see the data. For example, access to personal employee information should only be for payroll or benefit purposes. Be sure that relevant vendor agreements provide adequate safeguards and that vendors agree to:

- abide by your company's security measures;
- cover the costs and take all action required to rectify any misuse or loss of sensitive data;
- have the financial capability, whether through a bond or insurance coverage, to pay for any required remediation in case of information loss.

Screen all employees

Implement hiring practices for all employees, especially those with access to sensitive information. Use criminal and background screening companies.

Establish and enforce privacy guidelines

All employees in a position to see or retrieve sensitive information – including cleaning crews, technicians, administrative assistants and temporary employees – should sign a confidentiality and security document.

Distribute and explain data protection protocols to all employees (clean desk policy, restricted access to data, visitor guidelines, etc.). Review and revise these practices on a regular basis, at least once a year. Retrain staff when protocol changes are made.

Set up a routine audit program

Put best practices and industry standards enforced by policies in place. Routinely audit them by making sure:

a) sensitive data is protected when not in use;

b) only authorized users can access confidential information;

c) sign-in logs are being maintained and sensitive documents are being properly destroyed.

Limit the use of portable technology

Restrict the transfer of sensitive information from on-premises computers to portable devices, such as cellphones, tablets, laptops, backup tapes, USB keys and removable hard drives. If any confidential data must be transferred to these devices, make sure information is encrypted and protected with a strong password.

Delete the sensitive information from these devices as soon as it is no longer needed or is transferred to other non-portable devices for retention.

Don't use unsecured wireless networks

Off-the-shelf wireless networks do not provide adequate enterprise-level security to safeguard confidential data. Ensure that the wireless network you use includes strong authentication and secure communication.

Ensure that remote access to your network is secure

Remote access to your network should be made through appropriately enabled Virtual Private Network (VPN). All default passwords to your network must be changed regularly.

Utilize password protection and encryption

Always encrypt sensitive information. Inexpensive encryption technologies are readily available. All system users should be assigned unique user names and strong passwords, changed at least quarterly. Conduct a password audit annually.

Protect yourself against malware

To reduce the risk that your network could be infected by harmful software:

1. Protect your network with an antivirus program that includes a firewal.
2. Analyze the network regularly to detect threats.
3. Restrict access to websites that could transmit malware.
4. Never click on a link and never download a file from a source not identified as trustworthy (emails, unknown websites, etc.).

Update all your systems and software regularly

To maintain the best possible protection, always download and install the latest system and security patches and updates for all your software programs and applications.

Properly dispose of technology hardware

Implement policies on how to securely destroy old computers, disks, tapes, copy machines, printers, scanners, CDs, memory devices and any other equipment that may contain sensitive information (similar practices should be used to properly dispose of sensitive data that is paper-based). Often these devices can provide access to data, even after the information has been deleted. Do not rely on the "delete" or "trash" function to remove files containing sensitive information. It is often best to physically destroy the devices and any memory units when they are no longer needed.

Call your broker – your best source for information and advice.

INTERESTED IN LEARNING MORE ABOUT WHAT YOU CAN DO TO PROTECT YOUR BUSINESS?
YOUR INSURANCE BROKER CAN ADVISE YOU.

https://www.priv.gc.ca/en/privacy-topics/privacy-policies/02_05_d_56_tips2/
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/