Privacy tips for small businesses

Big or small all businesses need to keep privacy and security in mind. Help protect yourself, your employees, and customers/clients by following these tips!

1. Keep software and devices up to date and protected

Ensure all devices and software are kept updated and password protected. Invest in Next-Gen antivirus software as it helps in the defence against viruses and malware.

2. Secure wi-fi and provide firewall security for internet connections

If you have a Wi-Fi network for your workplace, make sure it is secure, encrypted, and hidden. In addition, ensure your operating system's firewall is enabled, employees that work from home are protected, and a virtual private network (VPN) is established in order to help protect your internet connection and business.

3. Make backup copies of important data and information

Regularly backup data on all devices. This can be automatically or manually done and store the copies either on an offsite location in Canada or the applicable privacy jurisdiction or in the cloud.

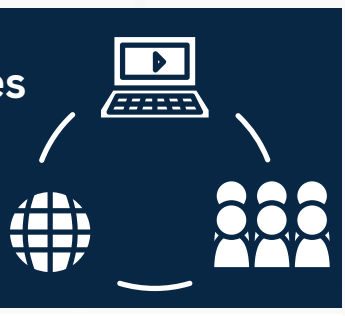
4. Protect personally identifiable information (PII)

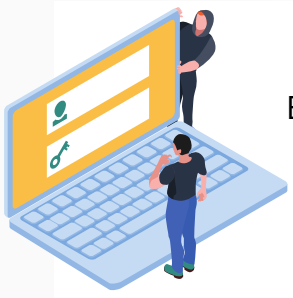
When collecting, using, and disclosing PII it is important to protect information by being aware of legislation, policies, practices, having conversations with employees, and keeping everyone involved informed. In addition, limit employee access to install software and to only data and information necessary to perform their job duties.

- PII is any type of data that can be used to identify someone such as their name, address, date of birth, employment history, etc.

5. Train employees in security and privacy principles

Establish basic practices and policies for employees, such as requiring strong passwords, establish appropriate Internet use guidelines, set rules describing how to handle and protect customer information and other vital data.





6. Have strong passwords and authentication

Ensure employees use strong unique passwords which are changed periodically and consider implementing multi-factor authentication that requires additional information beyond a password to enter accounts and systems.

7. Control physical access to your computers and create user employee accounts

Ensure employees working from home have distinct work computers to separate personal use of devices. Prevent access or use of business computers by unauthorized individuals and ensure separate user accounts are created for each employee.

8. Employ best practices for payments

Work with banking institutions or processors to ensure reliable and authenticate tools and anti-fraud services are being used and have a dedicated computer to process payments alone which and isolates payment systems from other programs. Follow the Payment Card Industry Data Security Standard with digital payment methods.

9. Update privacy and security training protocols and action plans

Establish a cyber security protocol and practices as having a protocol will make sure that staff use their devices safely, know their responsibilities and expectations, and allows for a uniform response and information that can be referred to.

- Require users to password-protect their devices, encrypt their data, and install security apps to prevent criminals from stealing information.
- Set reporting procedures for lost or stolen equipment.
- Have a clear privacy policy and terms of use for staff and customers.
- Conduct regular privacy and security audits.

10. Secure Corporate Mobile Devices

Restrict employee download access to only company-approved apps, require the use of complex pin codes, and restrict saving passwords devices.

DURHAM REGION

Access and Privacy Office
Legislative Services Division
Corporate Services Department
Privacy @durham.ca

If you require this information in an accessible format, please email the Accessibility Coordinator at accessibility@durham.ca or 905-668-4113 ext, 2009.