SMB Compliance Guide

Comprehensive breakdown of key regulations

INTRO

As a small or medium-sized business (SMB) operating in Canada or the United States, understanding and adhering to cybersecurity regulations is crucial for your success and longevity.

This guide will help you navigate the complex world of compliance in these markets, ensuring your business remains secure and avoids costly penalties.

01

Key Regulations *Canada/Us/International*

PIPEDA – Personal Information Protection and Electronic Documents Act
CPPA – Consumer Privacy Protection Act
CASL – Canada's Anti-Spam Legislation
DCIA – Digital Charter Implementation Act
PCI DSS – Payment Card Industry Data Security Standard
PROVINCIAL PRIVACY LAW

FTC – Federal Trade Commission Act
GLBA – Gramm-Leach-Bliley Act
HIPAA – Health Insurance portability and Accountability Act
PCI DSS – Payment Card Industry Data Security Standard
STATE REGULATIONS

GDRP – General Data Protection Regulation – European Union
ISO/EIC 27001 – Internation standard for information security management
CBPR – Cross Border Privacy Rules

STEP BY STEP
Compliance Check

02

1. Assess Your Regulatory Landscape

- ❑ Identify which regulations apply to your business based on location, industry, and data handling practices
- ❑ Create a list of all applicable regulations

2. Conduct a Comprehensive Data Audit

- ❑ Identify all types of data your business collects, processes, and stores
- ❑ Map data flows within your organization
- ❑ Determine where data is stored (on-premises, cloud, third-party processors)

3. Perform a Risk Assessment

- ❑ Identify potential vulnerabilities in your current systems and processes
- ❑ Assess the potential impact of data breaches or non-compliance
- ❑ Prioritize risks based on likelihood and potential impact

4. Develop and Implement Security Policies

- ❑ Create a comprehensive information security policy
- ❑ Develop specific policies for data handling, access control, and incident response
- ❑ Implement a data retention and destruction policy

5. Enhance Technical Security Measures

- ❑ Implement strong encryption for data at rest and in transit
- ❑ Set up robust access controls and authentication mechanisms
- ❑ Deploy and configure firewalls and intrusion detection systems
- ❑ Implement regular system and software updates

6. Establish a Privacy Program

- ❑ Appoint a privacy officer or team
- ❑ Create privacy notices for customers and employees
- ❑ Implement processes for handling data subject requests (access, deletion, etc.)

7. Conduct Employee Training

- ❑ Develop a comprehensive security awareness training program
- ❑ Conduct regular training sessions on compliance requirements and security best practices
- ❑ Implement a system to track and verify completion of training

8. Manage Third-Party Risks

- ❑ Create a vendor management policy
- ❑ Conduct due diligence on all third-party vendors
- ❑ Include appropriate security and compliance clauses in vendor contracts

9. Implement Continuous Monitoring and Auditing

- ❑ Set up systems for continuous monitoring of security controls
- ❑ Conduct regular internal audits of compliance measures
- ❑ Schedule periodic external audits or assessments

10. Develop an Incident Response Plan

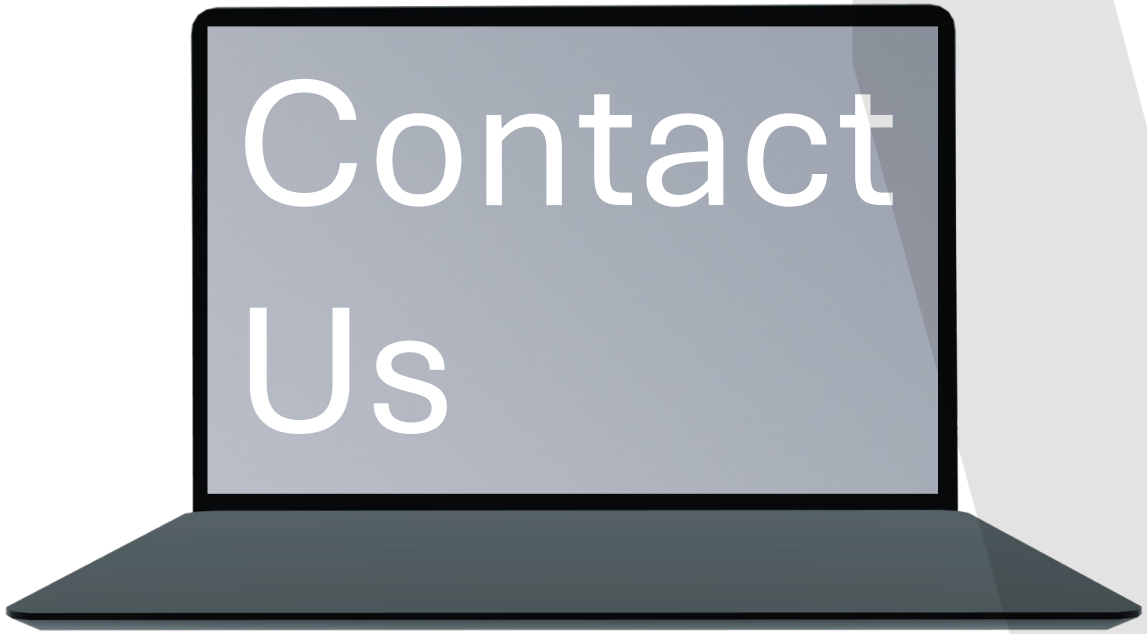
- ❑ Create a detailed incident response plan
- ❑ Assign roles and responsibilities for incident response
- ❑ Conduct regular drills to test the effectiveness of the plan

11. Establish Documentation Practices

- ❑ Implement a system for documenting all compliance efforts
- ❑ Maintain detailed logs of security incidents and responses
- ❑ Keep records of all privacy impact assessments and data processing activities

12. Continuous Improvement

- ❑ Schedule regular reviews of your compliance program
- ❑ Stay informed about changes in regulations and update your program accordingly
- ❑ Gather feedback from employees and stakeholders to improve your compliance efforts



Website
www.harkeco.com/hacktractive

Email
info@harkeco.com