PIPEDA Policy Requirements

Advised Policies for PIPEDA Compliance

TRUE NORTH

• PSR

Table of Contents

Policies List

- Privacy Policy (online)
- Vendor Management Policy
- Information Security Policy
- Access Control Policy
- Confidentiality Policy
- Email / Communication Policy
- Backup & Retention Policy
- Logging and Monitoring Policy
- Password Policy
- Encryption Policy
- Data Classification Policy
- Endpoint (Workstation) Policy
- Incident Response (IR) Policy
- Risk Management Policy
- Acceptable Use Policy (AuP)
- Change Management (CM) Policy
- Remote Access Policy
- Software Development Lifecycle (SDLC) Policy

Policy Summary Descriptions

Privacy Policy (online)

This is the customer-facing privacy policy (often also called a ‘privacy statement’) that organisations make available to the public on their website or app. It is especially important for meeting compliance requirements and maintaining a positive relationship with your customers through forward-thinking data protection practices.

PIPEDA principles 1, 2, 3, 8

Vendor Management Policy

Sets security requirements and controls for third-party service providers ("suppliers", or "vendors") to protect your company's data and systems.

PIPEDA principles 4, 5

Information Security Policy

A high-level policy governing the approach to information security management within the organization. A required document for many security standards, including ISO 27001 and SOC2.

PIPEDA principles 6, 7

Access Control Policy

Establishes what measures you're taking to appropriately govern employee access to your company's various information and systems.

PIPEDA principles 5, 7

Confidentiality Policy

This policy defines how your organization and employees will handle the confidential data of clients, business associates/partners, and/or the company itself. Clients expect the data you process or store on their behalf to remain secure, and this policy is an important part of ensuring that you deliver on that promise.

PIPEDA principles 5, 7

Email / Communication Policy

Sets the guidelines for using the organization’s communication mediums. It mentions what is acceptable and unacceptable for employees when communicating using the company’s devices, networks, email, etc.

PIPEDA principles 5, 7

Backup & Retention Policy

This document stipulates the criteria for determining how long data should be retained and the procedures for securely disposing of it once it is no longer needed.

PIPEDA principles 5, 7

Logging and Monitoring Policy

This document will list the log files you will collect and monitor. It also mentions what will be captured in those logs and what systems you must configure for logging.

PIPEDA principles 4, 5, 7

Password Policy

Defines the guidelines and requirements for using strong passwords (or passphrases). It mentions using password managers for different portals and includes a password expiration policy so employees regularly change passwords.

PIPEDA principle 7

Encryption Policy

Outlines the standards and practices for encrypting data to protect its confidentiality and integrity during storage and transmission.

PIPEDA principle 7

Data Classification Policy

Defines how to classify sensitive data by weighing the risk parameters. This ensures that the sensitive data is effectively handled according to the level of risk it poses to the organization.

PIPEDA principles 5, 7, 9, 10

Endpoint (Workstation) Security Policy

Defines rules and guidelines for securing the employees' workstations. This helps you reduce the risk of unauthorized access and data loss through workstation use.

PIPEDA principle 7

Incident Response (IR) Policy

A policy detailing the procedures and plans your company will use to respond to a security breach in accordance with applicable law. Most security and privacy standards (e.g., SOC2, ISO 27001) require this policy for effective incident management.

PIPEDA principles 1, 7

Risk Management Policy

A crucial component of an organization's overall risk management strategy. It outlines the company's approach to identifying, assessing, managing, and monitoring risks.

PIPEDA principles 5, 7

Acceptable Use Policy (AP)

Describes the acceptable and prohibited uses of the organization's IT resources by employees or users to ensure security and compliance.

PIPEDA principles 5, 7

Change Management Policy

Establishes the process for managing changes to IT systems and infrastructure to minimize risk and disruption, and achieve repeatable success by using standardized workflows.

PIPEDA principles 6, 7

Remote Access Policy

Provides guidelines and security measures for employees working remotely to maintain data security and productivity outside the office.

PIPEDA principles 5, 7

Software Development Lifecycle (SDLC) Policy

Details how you will build your software/application using secure coding practices. Typically, this policy will also detail the testing procedures your Dev team will use to ensure your company's development workflows meet the compliance requirements.

PIPEDA principles 4, 5, 9

What Now?

As you've navigated this guide, we hope you've gained a deeper understanding of the PIPEDA requirements and the value these policies could add to your organization's privacy practices. Embracing PIPEDA compliance is not just about meeting a regulatory requirement; it's about fostering trust in your services and protecting your customers' personal information – a fundamental aspect of data-driven business.

At True North PSR, we recognize that the path to PIPEDA compliance can seem challenging. If you determine that you don't have sufficient in-house resources to properly execute this project, this is where our expertise can make a crucial difference.

Our team is ready to assist you at every step, ensuring that your compliance efforts are as seamless and efficient as possible. By partnering with us, you gain access to a wealth of knowledge and a partner who is as committed to securing your customers' data as you are.

Consider visiting our website at <www.TrueNorthPSR.com> to learn more about how we can help streamline your compliance program, ease the burden on your internal teams, and enhance your privacy practices. We would be happy to help you turn the complexities of PIPEDA compliance into a strategic advantage for your business.