

Effective Privacy Documentation to Empower Your Organization

Regardless of whether you are a government ministry, agency, or part of the private sector, your organization's privacy documentation should clearly demonstrate a commitment to information protection. Putting well-designed privacy policies and procedures in place empowers an organization to create a trusting relationship with its customers/the public, and guides employees on how to handle information. Here is a quick summary of some of the pieces that should form your suite of privacy documentation:

Privacy Policy: The Privacy Policy is the centerpiece of your privacy documentation — it should provide a clear understanding of why you need to collect their personal information, how you safeguard it, and whom you share it with. This policy must clearly and succinctly outline how *you* comply with privacy best practices.

Employee Privacy Policy: When you respect your employees' rights and interests, you command their loyalty. Your employee privacy policy sends a clear message that safeguarding employee information is a priority to you. Equally important, the policy should indicate the limitations on your employees' privacy rights, e.g., the use of video surveillance and the monitoring of company resources (such as e-mail and Internet activity).

Web Site Privacy Policy: The Web Site Privacy Policy addresses the protection of personal information online and should clearly tell your Web site visitor how the information collected on the site will be used.

Privacy Breach Response Policy: This policy ensures a consistent approach when privacy is violated. A step-by-step guide helps your organization leap into action, minimize response time, and therefore mitigate the negative impact of the breach.

Employee Procedures for Safeguarding Personal Information: Implementing a formal procedure for safeguarding personal information internally guides your employees and contractors on how to manage privacy issues on a daily basis. The procedure should address, to name a few safeguards, securing one's unattended work environment; access controls; precautions to take when faxing or emailing information; secure disposal of records, escorting visitors; reporting lost security access cards; and laptop best practices.

Information Security Policies: Because security threats have increased exponentially over the past decade, securing systems from internal and external threats has become a priority in the public and private sectors. A good security policy dictates the scope, direction, and priority for security within an organization.

Others: **Work-at-Home Policy, De-identification Guidelines....**

Awareness is Critical

It is imperative that the adopted policies and procedures be consistent with daily practices, used as the basis for your training and audit initiatives, and reviewed at least annually. If not, the potential disconnect will undermine your privacy program.

Our goal at PrivaTech Consulting is to empower organizations with tools to build a privacy-conscious environment and reduce privacy risks. For detailed templates for all the above documentation and more, visit www.privacyCD.com. Our samples are not industry or jurisdiction specific, but can be easily customized – they are simply intended to help you assess your existing documentation and fill in the gaps!

Fazila Nurani, B.A.Sc. (E.Eng.), LL.B., CIPP/C. Fazila is a privacy lawyer, consultant and trainer with PrivaTech Consulting. Fazila advises organizations in a wide range of industries on privacy best practices, compliance with data protection laws, and managing information security risks. She can be reached at fnurani@privattech.ca

www.privatech.ca
16 Northumberland Terrace
Thornhill, Ontario, Canada L3T 7E5

Phone: (905) 886 0751
Email: info@privatech.ca
Fax: (905) 886 9974