Private Sector Privacy Management Program Self-Assessment

How well is your organization protecting the privacy of your clients and customers?

The Office of the Information and Privacy Commissioner (OIPC) wants to help your organization meet your legal obligations and the expectations of your clients and customers for the privacy and security of their personal information.

Who we are
The Office of the Information and Privacy Commissioner provides independent oversight and enforcement of the *Personal Information Protection Act* (PIPA), which governs the collection, use, and disclosure of personal information by organizations.

Our goal
Our goal is to help your organization better manage personal information. Properly protecting that information is required by law, and it also builds trust in your organization. And that's great, so you can avoid privacy breaches and complaints. The best way to do so is to establish a program to manage the personal information you collect, use, and disclose. Our guidance, *Getting Accountability Right with a Privacy Management Program*, outlines simple safeguards for you to put in place to minimize privacy risks. Visit our website to download the guidance: https://www.oipc.bc.ca/guidance-documents/1435.

Take the self-assessment
Wondering if your organization has an effective privacy management program? We encourage you to take 15 minutes to complete the attached voluntary self-assessment form. Your results will help you decide whether improvements are needed to better protect the personal information your organization collects and to comply with the law.

More info
Check out our guidance documents at www.oipc.bc.ca/resources/guidance-documents. You can also review our PrivacyRight private sector education program, where you'll find webinars, videos, podcasts and other materials that will help ensure compliance with PIPA.

Questions?
Contact us at (250) 387-5629.

If you wish, you can send your completed form to us at info@oipc.bc.ca and we can discuss it with you.

Sincerely,

Michael Harvey
Information and Privacy Commissioner

Private Sector Privacy Management Program Self-Assessment

This tool can help you to identify areas in need of improvement in your privacy management program. Please review your organizations privacy-related policies and practices and rate them using a 5-point scale, where "1" indicates that the measure is not in place or has not been implemented at all and "5" indicates that the measure has been fully implemented. Any item ranked "3" or lower indicates that the measure requires immediate attention.

5pt Rating Scale 1 = not in place 5 = fully implemented	**Privacy Officer**
	1. A designated staff member is assigned to privacy matters.
	2. The privacy officer is equipped with the resources to do their job.
	3. Senior management support and promote privacy management.
Personal Information Inventory	
	4. Your organization maintains an inventory of the personal information collected that includes: • the types of personal information collected and who the personal information is about • the purpose for collecting, using or disclosing the information • the sensitivity of the information • where the information is stored
	5. The inventory is reviewed regularly and any needed revisions are made.
Privacy Policy	
Your organization has written *privacy policies that detail…*	
	6. Your organization's commitment to protect the personal information it collects.
	7. Your organization's intention to comply with PIPA.
	8. A definition of personal information.
	9. The types of personal information your organization collects.
	10. The purposes or reasons for collecting personal information.
	11. How your organization will obtain consent to collect personal information.
	12. That individuals have a right to withdraw consent.
	13. Limits on the use and disclosure of the personal information collected.
	14. That individuals have a right access their personal information.
	15. How an individual can access their personal information.
	16. How your organization will maintain the accuracy of personal information.
	17. Retention periods for storing personal information.
	18. How personal information will be destroyed after the retention period ends.
	19. Administrative, physical and technological security controls to protect personal information.
	20. Your organization's process for lodging and managing privacy complaints.
	21. Contact information for the privacy officer in your organization.

	22. A person's right to obtain assistance from OIPC.
	23. Mandatory reporting of suspected privacy breaches to the privacy officer or a senior manager.
Video and Audio Surveillance *(Complete this section only if your organization uses video or audio surveillance in any capacity)*	
	24. Less intrusive alternatives to surveillance were considered prior to installation of surveillance.
	25. To determine whether surveillance is still needed, your organization conducts regular reviews of (a) the issues surveillance is intended to prevent, (b) the frequency with which the issues occurs, (c) the ability of surveillance to prevent the issues, and (d) the sensitivity of personal information being collected.
	26. Your organization has written policy relating to the collection, use, disclosure and security of personal information captured by the surveillance system.
Staff Training & Education	
	27. The privacy policy (and surveillance policy, if applicable) is communicated to ALL employees.
	28. Regular training is provided to ALL staff on expectations regarding the collection, use, disclosure and protection of personal information.
	29. Participation in privacy training is mandatory.
	30. ALL staff are aware that they are required to report privacy risks, breaches and other issues to management.
Oversight of Service Providers and Contractors	
	31. Privacy provisions regarding collection, use, disclosure and security of personal information are clearly written into any contracts.
Risk Assessments & Security Safeguards	
	32. Conducts personal information assessments (PIAs) for new or amended/updated initiatives that involve the collection of personal information.
	33. Regularly reviews personal information holdings and the sensitivity of the personal information to determine appropriate safeguards needed to protect personal information.
	34. Employs administrative safeguards (i.e., privacy policies, training, confidentiality agreements, appropriate screening of contractors and new hires).
	35. Employs physical safeguards (i.e., paper files in locked cabinets, computer servers in locked rooms, no personal information left on desks, etc.).
	36. Employs technological safeguards (i.e., password protocols to access computer systems, mandatory encryption of USB or other storage devices, restrictions on personal mobile devices).
	37. Conducts regular reviews of its privacy policies and security safeguards.

For additional information or assistance, return this form to OIPC on a strictly confidential basis:

Office of the Information and Privacy Commissioner for British Columbia
PO Box 9038 Stn Prov Govt
Victoria BC V8W 9A4
info@oipc.bc.ca