Yukon Information and Privacy Commissioner

Privacy Management Program Self-Evaluation Tool

This tool is designed as a resource for public bodies[1] to 'self-evaluate' the maturity of their privacy management program. This tool can be used to increase maturity by identifying areas where more work is required to bring the program to full development. This tool is a companion to the 'Guidance for Public Bodies on Accountable Privacy Management', which contains a detailed description of the building blocks.[2]

A. PROGRAM BASICS

PROGRAM BUILDING BLOCK	PROGRAM ELEMENT	REQUIREMENT IN PLACE (YES, NO, PARTIAL)	COMMENTS
Public Body Commitment	**Executive support:** Is there a properly-resourced privacy management program?		
	Privacy officer: Has a privacy officer been appointed who is both at a senior level and responsible for (a) ensuring the public body is compliant with ATIPP and (b) managing and directing the privacy management program?		
	Reporting: Have reporting mechanisms been established within the public body to ensure that executive management is kept informed about (a) whether the program is functioning as expected and (b) breaches of privacy?		
Program Controls	**Personal information inventory:** Has the personal information in the custody or control of the public body been inventoried?		

[1] Under the *Access to Information and Protection of Privacy Act* (ATIPP).

[2] Located on the Yukon Information and Privacy Commissioner's website at: http://www.ombudsman.yk.ca/uploads/media/55f99c6eed395/Guidance Privacy Management - Revised Nov 2016.pdf?v1

	Policies and procedures: Have policies and procedures been documented and implemented to address the following: • how to meet the purpose of and exercise proper authority for the collection, use and disclosure of personal information; • how to meet the requirements for notification and consent; • how to ensure the accuracy of personal information; • how to facilitate access to and correction of personal information; • how personal information will be secured; • how a privacy breach will be managed; and • how complaints will be managed?		
	Risk assessment tools: Are privacy impact assessments (PIAs) and security threat risk assessments (STRAs) being conducted routinely for all new projects involving personal information, or for the new collection, use or disclosure of personal information?		
	Training: Does the public body have a privacy-awareness training program where employees receive training on the privacy policies and procedures at the start of their employment and annually thereafter?		
	Service provider management: Do service-provider contracts contain provisions that (a) clarify that the public body controls the personal information collected, used or disclosed under the contract and (b) allow the public body to effectively control the personal information in the custody of the service-provider, including breach management?		

	Does the public body monitor these contracts to ensure compliance?		
	Communication with individuals: Are communications, such as notices or notifications and forms and processes, being utilized to inform individuals about their privacy rights and the public body's program controls?		

B. ONGOING ASSESSMENT AND REVIEW

Assess/ Revise Program Basics	**Commitment:** Are privacy resources and reporting evaluated at least annually for effectiveness?		
	Controls: • Is the personal information inventory reviewed and updated as new personal information is added to it? • Are policies and procedures reviewed and updated at least annually? • Are risk assessments monitored and updated as new risks are addressed or as any risk is mitigated? • Is training evaluated and updated at least annually? • Are breach and incident-response protocols reviewed and updated at least annually? • Are service-provider management tools reviewed and updated at least annually? • Are external communication methods reviewed and updated, as needed, to address ineffective communication?		