SQUAMISH
HARDWIRED *for* ADVENTURE

Privacy Management Program

A. BUILDING BLOCKS

Organisational Commitment	**a) Executive Level Support**	Executive management of an organization is key to its successful Privacy Management Program and essential for its privacy respectful culture. The Executive Management of the District of Squamish is: • Committed to providing the resources necessary to develop, implement, assess and revise the Privacy Management Program • Responsible to designate and empower a privacy officer in the public body to be responsible for managing the Privacy Management Program and monitoring compliance with the FOIPP Act
	b) Privacy Officer	The privacy officer (or privacy designate) role is well-defined at the District of Squamish and is fundamental to the privacy decision-making process. Role and responsibilities of the Privacy Officer are clearly identified and communicated throughout the organization and includes the: • Development and implementation of 'program controls' and their ongoing assessment and revision • Development, delivery, and review of training, policies, and procedures • Ensure privacy protection is built into every major function involving the collection, use, or disclosure of personal information • Monitoring compliance with outlined 'program controls' and regular assessment and revision of programs as necessary • If the monitoring process uncovers a problem, the appropriate official will document and address concerns

	c) Privacy Office	Privacy office at the District of Squamish includes: • Privacy Head: Robin Arthurs • Privacy Coordinators: Charlene Pawluk, Chetan Kaur • Records Management Coordinator: Cass Strong • Manager of IT Security & Infrastructure : Eva Perez
	d) Reporting	Reporting mechanisms are clearly established and reflected in the District's program controls
Program Controls	**a) Personal Information Inventory**	Personal information is continuously monitored and updated to keep it current and to identify and evaluate new collections, uses, and disclosures of personal and sensitive information
	b) Policies	Privacy policies at the District of Squamish include: • District of Squamish Freedom of Information and Protection of Privacy Bylaw No. 2257, 2015 • Freedom of Information and Protection of Privacy Policy • District of Squamish Records and Information Management Policy • District of Squamish Records Retention and Disposal Bylaw No. 2622, 2019 These policies are reviewed and updated, following assessments or audits, in response to a breach or complaint, new guidance, industry-based best practices, or as a result of environmental scans
	c) Risk Assessment Tools	Risk assessment tools, such as Privacy Impact Assessments (PIAs) are used for new initiatives, as required. The risk assessment tools are further reviewed and updated on regular basis so that the privacy and security risks of changes or new initiatives within the organization are always identified and addressed

	d) Training and education requirements	Employees participate in recommended privacy awareness training as necessary to ensure awareness of the policies and procedures
	e) Breach and incident management response protocols	Privacy breaches are taken very seriously. Office of the Privacy Commissioner (OIPC) and parties involved are advised of the breach at the earliest. Incident management response protocols are reviewed and updated to implement best practices or recommendations and lessons learned from post-incident reviews
	f) Service Provider management	Procedures exist and are applied to manage personal information involved in service provider contracts
	g) External communication	It is ensured that all external communications meet the requirements of the FOIPPA, individuals are informed about their rights under the act and about the public body's complaint management process, and individuals are informed that they can contact the OIPC, if required

SQUAMISH
HARDWIRED *for* ADVENTURE

B. ONGOING ASSESSMENT AND REVISION

Oversight and Review Plan	**a) Develop an oversight and review plan**	A plan to review and revise the Privacy Management Program exists and includes: • A requirement that the program controls are assessed on an ongoing basis to mitigate risks to privacy protection • A requirement to conduct periodic or random audits on the effectiveness of the program controls • Revision of the program controls as required to mitigate the risks to privacy • Communication with employees about changes to the program controls
Assess and Revise Program Controls as Necessary	**a) Update personal information inventory** **b) Revise Policies** **c) Keep the risk assessment tools updated** **d) Modify training and education** **e) Adapt breach and incident response protocols** **f) Fine-tune service provider management** **g) Improve external communication**	The review is carried out in accordance with the revision of the program controls as necessary