Checklist of PMP requirements for public bodies

The following checklist can help public bodies meet the requirements for privacy management programs (PMP) as set out in *Protection of Privacy Act* (POPA) and supplements OIPC Guidance on PMPs.

Requirements for all public bodies (see POPA section 25, 10, and M-Reg section 6(1))

☐ **Designated Privacy Officer**: Identify or designate an individual responsible for ensuring the public body's compliance with the Act and regulations. Ensure that where necessary, authority is delegated from the head of the public body, to the Privacy Officer.

☐ **Documented internal policies & procedures**: Establish written rules addressing the public body's duties, including:

- ☐ **Access and correction**: Processes for responding to requests for personal information or requests for correction.
- ☐ **Privacy complaints**: A defined process for receiving and responding to complaints.
- ☐ **Privacy Incident response**: A policy and process for responding to breaches and notifying affected individuals in accordance with the Act and regulations
- ☐ **Non-personal data**: Policies for the creation, use, and disclosure of non-personal data (anonymized or synthetic data).
- ☐ **Automated systems**: Procedures for the use and safeguarding of personal information within automated systems (e.g., AI or algorithms).

☐ **Personal information inventory:** Create a personal information inventory which can be used to meet the requirements of the Act and regulations.

☐ **Security classification system**: Implement a system to classify personal information, derived data, and non-personal data based on sensitivity.

☐ **Safeguards:** Establish administrative, technical and physical safeguards for safeguarding and managing personal information.

☐ **Mandatory employee training:** Ensure all employees and contractors undergo regular training to understand their obligations under the Act.

☐ **Periodic review cycle**: Establish specific timelines for the regular review and assessment of the PMP to ensure it remains effective.

☐ **Public transparency:** Establish a process to make the PMP documentation available to the public upon request or by default (e.g. published on website).

Enhanced Requirements for public bodies that process sensitive personal information or high volumes of personal information

(see M-Reg section 6(2))

The additional requirements to include policies and procedures for certain activities, and the public body's duties regarding these activities, apply if the public body manages a high volume of personal information or highly sensitive information:

☐ **Define accountability**: Document the public body's internal privacy management structure. Clearly document the roles, responsibilities, and accountabilities of all employees in relation to the public body's obligations under the Act.

☐ **Privacy Impact Assessment (PIA) process:** Document policies and procedures for creation and ongoing management (updating as needed) of PIAs for new programs and activities or substantial changes to existing ones including for submitting the PIAs to the OIPC.

☐ **Policies and procedures for proactive monitoring of information:** Document policies and procedures setting out how the public body actively monitors systems holding personal information, data derived from personal information or non-personal data, to assess security measures and mitigate risks.

☐ **Consent documentation**: Document policies and procedures to ensure consent, written, oral or electronic, is obtained in accordance with POPA and its regulations.

☐ **Employee and third-party oversight**: Define the roles, responsibilities and accountabilities of employees (which in POPA include third-party contractors and service providers) of the public body in relation to the public body's obligations under the Act.

☐ **Policies for high-risk uses**: Establish policies and procedures related to the use of personal information in artificial intelligence systems, the creation of data derived from personal information and the creation of non-personal data.

☐ **Safeguards:** Establish written administrative, technical and physical safeguards for managing personal information, data derived from personal information and non-personal data.