Privacy Breach Response Protocol

A **privacy breach** includes the loss of, unauthorized access to, or unauthorized collection, use, disclosure, or disposal of personal information.

The Office of the Registrar of Lobbyists (ORL) is a public body under the *Freedom of Information and Protection of Privacy Act (FIPPA)* and is required to protect the personal information in its custody or under its control as contemplated by section 30 of the Act that states:

A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

Accountable privacy management[1] includes program controls to ensure that FIPPA's requirements are met, for example, our privacy breach management response protocol.

This protocol outlines the steps the ORL takes to manage known or suspected privacy breaches and is based on the Office of the Information and Privacy Commissioner's privacy breach management guidelines.[2] The Privacy Officer[3] is responsible for the coordination, investigation, and resolution of breaches under this protocol.

Step 1: Report and contain

Employees are required to report all breaches, and suspected breaches, to their supervisor who will report the breach to the Privacy Officer. If the Privacy Officer is unavailable, the supervisor will manage the breach. If the supervisor is unavailable, employees should inform the Privacy Officer.

---

[1] *Accountable Privacy Management in BC's Public Sector* (https://www.oipc.bc.ca/guidancedocuments/1545)

[2] *Privacy Breaches: Tools and Resources* (https://www.oipc.bc.ca/guidance-documents/1428)

[3] The Deputy Registrar is the ORL's Privacy Officer

The Privacy Officer will take immediate steps to contain the breach, including seeking support from Information Technology (the systems team) to:

- stop unauthorized practice;
- recover records;
- shut down the system that was breached;
- revoke or change computer access codes;
- correct physical security weaknesses.

The Privacy Officer will update the Executive and management about breaches and will liaise with the senior communications manager regarding media statements, if required.

Step 1a: Document breach

The Privacy Officer, supervisor, or employee will complete a breach reporting form to document the breach and the steps of the breach management process as they occur, including:

- number of affected individuals;
- type of personal information involved;
- cause and extent of breach;
- containment efforts;
- risk evaluation;
- notification;
- prevention strategies and security safeguards.

Step 2: Risk evaluation

The Privacy Officer or supervisor must complete a risk evaluation to understand whether affected individuals should be notified.

Evaluating the risks includes considering the personal information involved, the number of affected individuals, the cause and extent of the breach, and the foreseeable harm from the breach.

The Privacy Officer will determine if a breach could reasonably be expected to cause significant harm to affected individuals. The privacy officer, supervisor, or employee will notify affected individuals if the breach could reasonably be expected to cause them significant harm.

The risk evaluation process, including decisions regarding whether or not to notify, should be documented.

Step 3: Notification

If individuals have to be notified, the Privacy Officer, supervisor, or employee will do so as soon as possible by phone, letter, or in person. They will not make

direct contact if this could cause further harm, is cost prohibitive, or the contact information is unavailable.

Notification of affected individuals will include:

- date of the breach;
- description of the breach;
- description of the personal information involved;
- risk(s) to the individual;
- steps taken to control or reduce the harm;
- future steps planned to prevent further privacy breaches;
- steps the individual can take to control or reduce the harm; and
- contact information of the ORL's Privacy Officer.

Step 4: Security safeguards and prevention strategies

The Privacy Officer, supervisor, or employee will determine whether any improvements or changes to security safeguards are needed as a result of the breach, including whether additional preventative measures are needed. For example:

- Audit of physical or technical security;
- Root cause analysis;
- Revisiting or developing internal policies and procedures; and
- Additional training.

The Privacy Officer will ensure that an annual proactive assessment of the ORL's security safeguards (administrative, physical, and technical) is done to ensure the ORL is compliant with section 30 of FIPPA.