Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

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 Information and Privacy Commissioner ("OIPC") is a public body under FIPPA and as such is required to protect the personal information in its custody or under its control as contemplated by section 30 of the *Freedom of Information and Protection of Privacy Act* (FIPPA).

Section 30 of FIPPA 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 in respect of personal information protection are met. One such program control is a privacy breach management response protocol.

This protocol outlines the steps the OIPC takes in managing known or suspected privacy breaches (breaches) and is based on the OIPC's privacy breach management guidelines.[2] The Privacy Officer[3] is responsible for the coordination, investigation and resolution of breaches under this protocol.

Step One: Report and Contain

A breach should immediately be reported to one's supervisor.

The Supervisor will report the breach to the Privacy Officer. If the Privacy Officer is unavailable, the Supervisor will assume the role of Privacy Officer for the purposes of managing the breach.

---

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

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

[3] The Deputy Commissioner/Deputy Registrar is the OIPC's Privacy Officer

The Privacy Officer, Supervisor, and (designated) staff will take immediate steps to contain the breach, including seeking assistance from Information Technology (the systems team). For example:

- 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 keep the Executive apprised of any breaches and their management.

The Privacy Officer will liaise with the Information and Privacy Commissioner and the Director of Communications with respect to any public comments regarding a breach.

Step One A: Document Breach

The Privacy Officer, Supervisor, or designated staff will open a file and 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 Two: Risk Evaluation

The Privacy Officer, Supervisor, or designated staff will, within two days of discovering the breach, conduct a risk evaluation to determine 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[4].

Affected individuals must be notified 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.

[4] See Step 2: Evaluate the risks in the OIPC's *Privacy Breaches: Tools and Resources* for further information on risk evaluations.

Step Three: Notification

If notification is to occur, it should occur as soon as possible after discovering the breach and no later than one week thereafter unless notification should be delayed in order to not impede a criminal investigation.

The Supervisor or designated staff should notify affected individuals directly (by phone, by letter, or in person) unless direct notification could cause further harm, is cost prohibitive or contact information is not available.

Notification of affected individuals should 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;
- Contact information of the OIPC's Privacy Officer

Step Four: Security Safeguards and Prevention Strategies

The Privacy Officer, Supervisor, or designated staff will assess whether the OIPC's security safeguards (administrative, physical and technical) are compliant with section 30 of FIPPA.

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

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