

Privacy Breach Response Protocol

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

The Office of the Information and Privacy Commissioner (OIPC) is a public body under the *Freedom of Information and Protection of Privacy Act* (FIPPA). Under section 30 of FIPPA, the OIPC is required to protect the personal information in its custody or under its control.

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 management¹ includes program controls to ensure that FIPPA's requirements for 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 Officer³ is responsible for the coordination, investigation, and resolution of breaches under this protocol.

Step 1a: Report and contain

Employees are required to report all breaches to their supervisor, including suspected breaches. 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. If the Supervisor is unavailable, employee should report directly to the Privacy Officer.

If the Employee has not already taken immediate steps to contain the breach, then the Privacy Officer, Supervisor, and Employee will take steps to contain the breach,

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

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

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

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

Step 1b: 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 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 breach⁴.

The Privacy Officer will determine if a breach could reasonably be expected to cause significant harm to affected individuals. The Privacy Officer, Supervisor, or designated staff 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.

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

Step 3: Notification

If the risk evaluation suggests affected individuals should be notified, the Privacy Officer, Supervisor, or Employee will do so as soon as possible after discovering the breach.

The Privacy Officer, Supervisor, or Employee will notify affected individuals directly (by phone, letter, or in person) unless direct notification 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 OIPC'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 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; and
- Additional training.

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

ADMINISTRATIVE POLICIES AND PROCEDURES	
Office of the Information and Privacy Commissioner	
Subject: Privacy Breach Response Protocol	Date Issued: March 3, 2016
Policy Number: 2.3	Last Revision: March 6, 2019