OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER FOR BRITISH COLUMBIA

O.R.L. office of the registrar of lobbyists BRITISH COLUMBIA

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. Common examples of actions that cause breaches include misdirected emails containing personal information, intentional, unauthorized access to personal information (also called "snooping"), intentional unauthorized ingress of computer systems (also called "hacking"), unintentional exfiltration of information as a result of employees being deceived through social engineering (for example, phishing), and lost or stolen documents.

The Office of the Information and Privacy Commissioner (OIPC) and the Office of the Registrar of Lobbyists (ORL) are public bodies under the *Freedom of Information and Protection of Privacy Act* (FIPPA). Under section 30 of FIPPA, the OIPC and ORL are 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 management[1] 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 and the ORL take 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 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.

---

[1] Accountable Privacy Management in BC's Public Sector, 2023: https://www.oipc.bc.ca/guidancedocuments/1545.
[2] Privacy breaches: tools and resources for public bodies, 2023: https://www.oipc.bc.ca/documents/guidance-documents/2584
[3] The Deputy Commissioner/Deputy Registrar is the Privacy Officer for the OIPC and ORL.

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, 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 breach[4].

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.

---

[4] See Step 2: Evaluate the risks in the OIPC's privacy breaches: tools and resources for public bodies for further information on risk evaluations.

STEP 3: NOTIFICATION

FIPPA requires public bodies to notify an individual and report to the Commissioner when a breach could reasonably be expected to result in significant harm to the affected individual. When this threshold is met, public bodies must carry out notification without unreasonable delay. FIPPA does not require the OIPC to report breaches to itself. However, with respect to affected individuals, the OIPC follows its guidance to all public bodies on risk analysis and notification assessment.

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, unless the OIPC determines that one of the two circumstances where FIPPA does not require notification applies. Section 36.3(3) sets out two circumstances when a public body is not required to notify affected individuals, even when the obligation to notify is triggered under s. 36.3(2):

- situations where the notice can be reasonably expected to result in immediate and grave harm to the affected individual's safety or physical or mental health, or
- if the notice can reasonably be expected to threaten another individual's safety or physical or mental health.

If notification if required, the Privacy Officer, Supervisor, or Employee will notify affected individuals directly (by phone, letter, or in person) unless direct notification is cost prohibitive, or the contact information is unavailable. Notification of affected individuals will include:

- Date of the breach (if known) or the date it came to the attention of OIPC/ORL
- Description of the breach, including if known a description of the personal information involved;
- Known or potential 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 actual or anticipated harm; and
- Contact information of the OIPC/ORL 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 and the ORL's security safeguards (administrative, physical and technical) is undertaken to ensure the OIPC and the ORL are compliant with section 30 of FIPPA.

ADMINISTRATIVE POLICIES AND PROCEDURES **Office of the Information and Privacy Commissioner and** **Office of the Registrar of Lobbyists**	
Subject: Privacy Breach Response Protocol	**Date Issued**: March 3, 2016
Policy Number: 2.3	**Last Revision**: April 8, 2026