

Ministry of Citizens' Services
Policy and Procedure for Public Bodies
Responding to Privacy Breaches

(Updated October 30, 2009)

1. Definitions

1.1 In this document:

“**FOIPP Act**” means the *Freedom of Information and Protection of Privacy Act* (RSBC 1996);

“**ministry**” or “**ministries**” means a ministry or ministries, as they may be, of the government of British Columbia;

“**OGCIO**” means the Office of the Government Chief Information Officer for British Columbia;

“**OIPC**” means Office of the Information and Privacy Commissioner for British Columbia;

“**personal information**” means “personal information” as defined in the FOIPP Act;

“**privacy breach**” has the meaning described in paragraph 2.1;

“**public body**” means a public body as defined in the FOIPP Act (and includes ministries);

“**record**” means “record” as defined in the FOIPP Act.

2. What is a Privacy Breach?

2.1 A privacy breach is a collection of, use of, disclosure of, access to, disposal of, or storage of personal information, whether accidental or deliberate, that is not authorized by the FOIPP Act.

3. Purpose

3.1 This document sets out the steps that ministries must follow, and that other public bodies are advised to follow, when responding to a privacy breach.

3.2 While this document most directly deals with privacy breaches that occur as a result of a loss or theft of personal information, it applies to all privacy breaches.

4. Policy

4.1 Public bodies must determine if personal information is involved when they become aware of an incident, occurrence or other event that could reasonably involve a privacy breach. For example, the loss, accidental disclosure or theft of information, computers, or other electronic devices. [If no personal information is involved, a privacy breach under this policy has not occurred; however it might be advisable to consider if other policies need to be considered (e.g. policies relating to security breaches).]

- 4.2 Public bodies must respond immediately to privacy breaches by following all the steps in the procedure that are relevant to the privacy breach. Immediate action will include any steps that can be taken to prevent further harm and to demonstrate that the public body has exercised due diligence in addressing the breach.

5. Procedure

- 5.1 All known or suspected privacy breaches require immediate remedial actions no matter the level of sensitivity of the personal information. Given the diversity of public bodies and the varied nature of privacy breaches, no “one-size-fits-all” response is possible or practical. Public bodies will need to tailor their actions to ensure they are proportional and appropriate to each privacy breach.
- 5.2 The following steps must be taken by public bodies for all privacy breaches. *As the circumstances for each privacy breach will vary, these steps might occur concurrently or in quick succession, and do not necessarily need to follow the order given below.*

A. CONTAIN THE BREACH

- Take immediate action to contain the breach and to limit its impact. Appropriate actions will depend on the nature of the breach and may include:
 - Isolate or suspend the activity that led to the breach
 - Disconnect the network cable from the system that was breached (do not power down or log off) and immediately contact WTS - IT Security Operations Branch, Investigations Unit for instructions on how to proceed;
 - Correct all weaknesses in physical or electronic security, including revoking or changing computer access codes as necessary;
 - Take immediate steps to recover the personal information, records or equipment from all sources, where possible;
 - Determine if any copies have been made of personal information that was breached, and recover where possible.

B. ASSESS THE EXTENT AND IMPACT OF THE BREACH

- This evaluation will form the basis for the actions the public body should undertake following the breach.
 - (i) Personal Information Involved**
 - What personal information has been breached?
 - Is the information sensitive? For example health information, social worker case histories, social insurance numbers, financial information or information that can be used for identity theft. A combination of personal information is typically more sensitive than a single piece of personal information.
 - (ii) Cause and Extent of the Breach**
 - What was the cause of the breach?
 - What programs and systems are involved?
 - Is the personal information encrypted or otherwise not readily accessible?
 - Has the personal information been recovered?
 - What steps have already been taken to minimize the harm?
 - Is this a one-time occurrence or an ongoing problem?

(iii) Individuals Affected by the Breach

- Who is affected by the breach? For example, employees, public, contractors, clients, service providers, other organizations.
- How many individuals are, or are estimated to be, affected by the breach?

(iv) Foreseeable Harm from the Breach

- What possible use is there for the personal information? Can the information be used for exploitation, fraud or other harmful purposes?
- Who is in receipt of the personal information? For example, a stranger who accidentally receives personal information and voluntarily reports the mistake is less likely to misuse the information than an individual suspected of criminal activity.
- Is there a relationship between the unauthorized recipient(s) and the data subject(s)? A close relationship between the two might affect the likelihood of harm.
- Is there a risk of significant harm to the individual as a result of the breach? For example:
 - security risk (e.g. physical safety)
 - identity theft or fraud
 - access to assets or financial loss
 - loss of business or employment opportunities
 - breach of contractual obligations
 - hurt, humiliation, embarrassment, damage to reputation or relationships
- Is there a risk of significant harm to the public body or organization as a result of the breach? For example:
 - loss of public trust in the public body
 - loss of assets
 - financial exposure
 - loss of contracts or business
 - risk to public health
 - risk to public safety

C. REPORT TO APPROPRIATE PARTIES

- Immediately notify:
 - For all privacy breaches involving a ministry (or ministries), the Knowledge and Information Services Branch of the OGCI. Ministries will provide the following information to the Knowledge and Information Services Branch:
 - date the breach was discovered;
 - nature of the breach;
 - individuals or entities notified about the breach;
 - and whether the situation is contained.

The Knowledge and Information Services Branch will determine if it will work with the ministry on the breach, based on the following considerations:

- the breach involves multiple ministries;
- the breach involves sensitive personal information;
- there is, or could have been, a reasonable expectation of harm to any individuals as a result of the breach;

- individuals will be, or have been, notified that their personal information was breached;
- the breach will be, or has been, reported to the Office of the Information and Privacy Commissioner; or
- whether the breach has a serious or potentially serious public impact.

The Knowledge and Information Services Branch will follow up with the ministry as necessary. If it determines it does not need to work with the ministry, it will refer the privacy breach to the Information Access Operations Branch of Shared Services.

- If the privacy breach does not involve a ministry, notify the FOIPP coordinator or other delegated person responsible for the administration of the FOIPP Act and / or privacy in the public body.
- The following should also be notified, as applicable:
 - The Information Security Branch of the OGCI as necessary, if a ministry, or the person responsible for security within the public body.
 - Senior staff of your public body, as necessary.
 - The police or other law enforcement authorities if the privacy breach involves theft or other potential criminal activity.
 - Building security or administration, if the breach was the result of a compromise of building security.

D. DOCUMENT THE BREACH AND CORRECTIVE ACTION

- Document the privacy breach in detail, including:
 - what happened and when
 - how and when the breach was discovered
 - the personal information involved and scope of the breach
 - who was involved, if known
 - individuals interviewed about the breach
 - whether the breach has been contained and any lost personal information retrieved
 - who has been notified
 - what corrective action was taken, including any steps the public body has taken to assist the individual in mitigating harm (for example providing credit watch services if appropriate)
 - recommendations including the corrective action that still needs to be taken.
- Ensure that evidence of the privacy breach is preserved.

E. CONSIDER NOTIFYING THE AFFECTED INDIVIDUAL

- Review the impact of the privacy breach to determine if notification of the individual, whose information has been breached, is appropriate.
- Consider if harm would come to a third party from the notification of the individual (e.g. a law enforcement agency.)

(i) Notifying affected individuals

- The key consideration in deciding whether to notify an affected individual should be whether notification is necessary to avoid or mitigate harm to an individual.
- Other considerations in determining whether to notify individuals include:

- Legislative requirements for notification
- Contractual obligations that require notification
- A risk of identity theft or fraud (usually because of the type of information that has been compromised such as SIN, banking information, identification numbers)
- A risk of physical harm (for example if the compromised information puts an individual at risk of stalking or harassment)
- A risk of hurt, humiliation or damage to reputation (for example when the compromised information includes medical or disciplinary records, criminal histories or family case files)
- A risk to business or employment opportunities.
- A risk of loss of confidence in the public body and/or good customer/client relations dictates that notification is appropriate.

(ii) When and how to notify

- If it is determined that notification of individuals is appropriate:
 - **When:** Notification should occur as soon as possible following the breach. (However, if you have contacted law enforcement authorities, you should find out from those authorities whether notification should be delayed in order not to impede a criminal investigation.)
 - **How:** Affected individuals should be notified directly – by phone, e-mail, letter or in person – whenever possible. Indirect notification using general, non personal information, should generally only occur when direct notification could cause further harm, is prohibitive in cost or contact information is lacking. Using multiple methods of notification – website publication, posted notices, media – in certain cases may be the most effective approach.

(iii) What should be Included in the notification

- Notifications should include the following information, as appropriate:
 - Date of the breach
 - Description of the breach (extent)
 - Description of the information compromised
 - Risk(s) to individual caused by the breach
 - Steps taken to mitigate the breach and any harms
 - Next steps planned and any long term plans to prevent future breaches
 - Steps the individual can take to further mitigate the harm or steps the public body has taken to assist the individual in mitigating harm. For example, how to contact credit reporting agencies to set up a credit watch, or information explaining how to change a personal health number or driver's licence.
 - Contact information of an individual within the public body or organization who can answer questions or provide further information
 - The right to complain to the Office of the Information and Privacy Commissioner and the necessary contact information. If the public body has already contacted the Commissioner's office, include this detail in the notification letter.
- Notifications should not include the following information:
 - Personal information about others or any information that could result in a further privacy breach
 - Information that could be used to circumvent security measures

- Information that could prompt a misuse of the stolen information (for example, if hardware was stolen for simple 'wiping and resale' but the breach notification prompts someone to realize that personal information is on the hardware and could be of some value if accessed)

F. INFORM OTHER PARTIES AS APPROPRIATE

- Inform other affected parties as appropriate, which may include the following:
 - **Office of the Information and Privacy Commissioner:** The following factors are relevant in deciding whether to report a breach to the OIPC:
 - The sensitivity of the personal information
 - Whether the breached information could result in identity theft or other harm, including pain and suffering or loss of reputation
 - A large number of people are affected by the breach
 - The information has not been fully recovered
 - The breach is the result of a systemic problem or a similar breach has occurred before

The OIPC may choose to undertake a further investigation.

To notify the Information and Privacy Commissioner, complete the Privacy Breach Notification Form located at

[http://www.oipc.bc.ca/forms/Privacy_Breach_Form_\(Dec_2006\).pdf](http://www.oipc.bc.ca/forms/Privacy_Breach_Form_(Dec_2006).pdf).

- **Public Affairs Bureau:** Notify the Public Affairs Bureau (this requirement is for ministries only) or your communications officer.
- **Insurers, professional or other regulatory bodies, third party contractors, internal business units, unions or others:** If required by contractual or other obligations, provide the information required, and include the information necessary to mitigate the harm caused by the breach.

G. PREVENT FUTURE BREACHES

- Thoroughly investigate the cause of the breach. This could require an audit of physical and technical security, as well as practices related to the administration of the personal information such as its collection, use, disclosure, storage and disposal.
- Examine safeguards, policies and processes and revise them if/where necessary to reflect lessons learned from the breach and to prevent potentially similar occurrences.
- After an appropriate period, review the effectiveness of the new policies and procedures. Modify them as needed.
- Provide all staff, including operational and administrative staff, with ongoing education on privacy issues to reduce the potential of future occurrence. In particular, provide training related to the nature of the breach.
- Provide privacy breach training as part of new employee orientation and provide annual updates for employees and contractors.

RESOURCES

1. Province of British Columbia

The FOIPP Act 'Policy and Procedures Manual'

<http://www.cio.gov.bc.ca/services/privacy/manual/default.asp>

The Core Policy and Procedures Manual, Chapters 12 and 15, and Chapter 12 Supplemental

http://www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm and

<http://www.cio.gov.bc.ca/prgs/cpm12.pdf>

Information Security Policy

<http://www.cio.gov.bc.ca/services/security/ISP.asp/>

2. Office of the Privacy Commissioner of Canada

'Key Steps for Organizations Responding to Privacy Breaches'

http://www.privcom.gc.ca/information/guide/2007/gl_070801_02_e.asp

'Privacy Breach Checklist'

http://www.privcom.gc.ca/information/guide/2007/gl_070801_checklist_e.asp

3. Office of the Information and Privacy Commissioner for British Columbia

'Key Steps in Responding to a Privacy Breach'

http://www.oipc.bc.ca/sector_public/resources/index.htm

'Privacy Breach Reporting Form'

http://www.oipc.bc.ca/sector_public/resources/index.htm

'Breach Notification Assessment Tool'

http://www.oipc.bc.ca/sector_public/resources/index.htm

ACKNOWLEDGEMENT

The Ministry of Citizens' Services thanks the OIPC for its permission to use its 'Key Steps in Responding to Privacy Breaches' in the development of this document.