Process for Responding to Privacy Breaches

1. Purpose

1.1 This document sets out the steps that ministries must follow when responding to a privacy breach. It must be read in conjunction with the Information Incident Management Process, which says:

1. The Government Chief Information Officer is responsible for the coordination, investigation, and resolution of information incidents.

2. All actual or suspected information incidents must be reported immediately to your supervisor and to the Government Chief Information Officer, using the Information Incident Management Process.

3. The Government Chief Information Officer is solely responsible for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach.

If there is inconsistency between the Information Incident Management Process and this document, the Information Incident Management Process prevails.

2. What is a Privacy Breach and What is an Information Incident?

2.1 A **privacy breach** is a collection, use, disclosure, access, disposal, or storage of personal information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act*.

A privacy breach is a type of information incident. **Information incidents** occur when unwanted or unexpected events that threaten privacy or information security. They can be accidental or deliberate and include the theft, loss, alteration or destruction of information.

Other **definitions** can be found in the Information Incident Management Process.

3. Process

3.1 All known or suspected privacy breaches require immediate remedial action, no matter the sensitivity of the personal information. Given the varied nature of privacy breaches, no "one-size-fits-all" response is possible, and actions are proportional and appropriate to each privacy breach.

3.2 The following steps are used to address privacy breaches. As the circumstances for each privacy breach vary, these steps might occur concurrently or in quick succession; they do not necessarily need to follow the order given below:

A. Report Immediately

- Employees, service providers or others must report suspected or actual privacy breaches immediately to their supervisor. The supervisor and/or employee, or other person also reports immediately to the Office of the Government Chief Information Officer (OCIO)by:

- Calling the Shared Services BC Service Desk at 250 387-7000 or toll-free at 1-866 660-0811 (available 24 hours a day); and
- Selecting Option 3 and requesting an "Information Incident Investigation".

Service providers must report to their Government contract manager, who in turn must report to the Office of the Government Chief Information Officer as above.

In all cases, the person who identifies a breach must make the call themselves if they are not able to reach a supervisor or other designated individual immediately.

This will invoke the Information Incident Management Process.

Privacy breaches must also be reported to the Ministry Chief Information Officer.

B. Contain the Privacy Breach

- Employees, business owners (including supervisors and service providers) or others should take immediate action to contain the privacy breach and to limit its impact. Appropriate actions will depend on the nature of the breach and may include:
  - Isolating or suspending the activity that led to the privacy breach;
  - Correcting all weaknesses in physical security;
  - Taking immediate steps to recover the personal information, records or equipment from all sources, where possible;
  - Determining if any copies have been made of personal information that was breached, and recovering where possible.

Note: Where the privacy breach involves information technology, the direction of the Investigations Unit must be sought before taking any containment steps.

C. Assess the Extent and Impact of the Privacy Breach

- As part of the Information Incident Management Process, business owners (including supervisors and service providers) or others will work with the OCIO Investigations Unit, Incident Response Lead, or others to determine the:

(i) Personal Information Involved

- What personal information has been breached?
- Is the personal information sensitive? Examples are 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

D. Document the Privacy Breach and Corrective Action Taken

- As part of the Information Incident Management Process, business owners (including supervisors and service providers) or others will work with the OCIO Investigations Unit, Incident Response Lead, or others to:

  1) ensure that evidence of the privacy breach is preserved; and

  2) document the privacy breach in detail, including:

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

E. Consider Notifying Affected Individuals

- The impact of privacy breaches must be reviewed to determine if it is appropriate to notify individuals whose personal information has been affected by the breach. As part of the Information Incident Management Process, the Incident Response Lead will work with the affected ministry so the ministry can notify affected parties and take other required actions, as appropriate.

(i) Notifying affected individuals

- The key consideration in deciding whether to notify an affected individual is whether it is necessary to avoid or mitigate harm to an individual, such as:
  - 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); or
  - A risk to business or employment opportunities.

- Other considerations in determining whether to notify individuals include:
  - Legislative requirements for notification;
  - Contractual obligations requiring notification;
  - 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 law enforcement authorities have been contacted, it may be appropriate to work with those authorities in order not to impede their investigation.)
  - **How**: Affected individuals should be notified directly – by phone, email, 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

- As part of the Information Incident Management Process, the Incident Response Lead will work with the affected ministry so the ministry can notify affected parties and take other required actions, as appropriate. Affected parties may include, for example: insurers, professional or other regulatory bodies, third-party contractors, internal business units, or unions.

- The Government Chief Information Officer is solely responsible for liaising with the Office of the Information and Privacy Commissioner regarding an actual or suspected privacy breach. The following factors are relevant in determining whether to report a privacy breach to the Office of the Information and Privacy Commissioner:
    - 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

G. Prevent Future Privacy Breaches

- Business owners (including supervisors and service providers) or others will work with the OCIO Investigations Unit, Incident Response Lead, or others to investigate and manage the privacy breach.
- Government, the ministry, or the ministry business owner will, as applicable, implement recommendations in accordance with the Information Incident Management Process.