Privacy Breach Reporting Protocol

What is the purpose of this protocol?

This protocol is designed to assist departments by defining processes to manage privacy breaches that are consistent across the government. This protocol will provide guidance on:

- Timelines when managing breaches;
- Determining risk of harm; and
- Notification, including who, when and how notification should occur.

What is a privacy breach?

A privacy breach, or information incident, is defined as the accidental loss or alteration, and unauthorized access, collection, use, disclosure or disposal of personal information or personal health information.

The most common privacy breaches occur when information of patients, clients or employees is stolen, lost or mistakenly disclosed. Some examples of privacy breaches are

- The loss or theft of equipment or devices that contain personal information;
- Emailing sensitive personal information outside of the government firewall;
- Faxes that go the wrong fax number;
- The storage of personal information and subsequent loss of a flash drive / USB stick or external hard drive which was not encrypted; or
- Snooping or browsing through information systems.

Guiding principles of this protocol

The principles listed below are intended to assist decision-makers when managing a privacy breach.

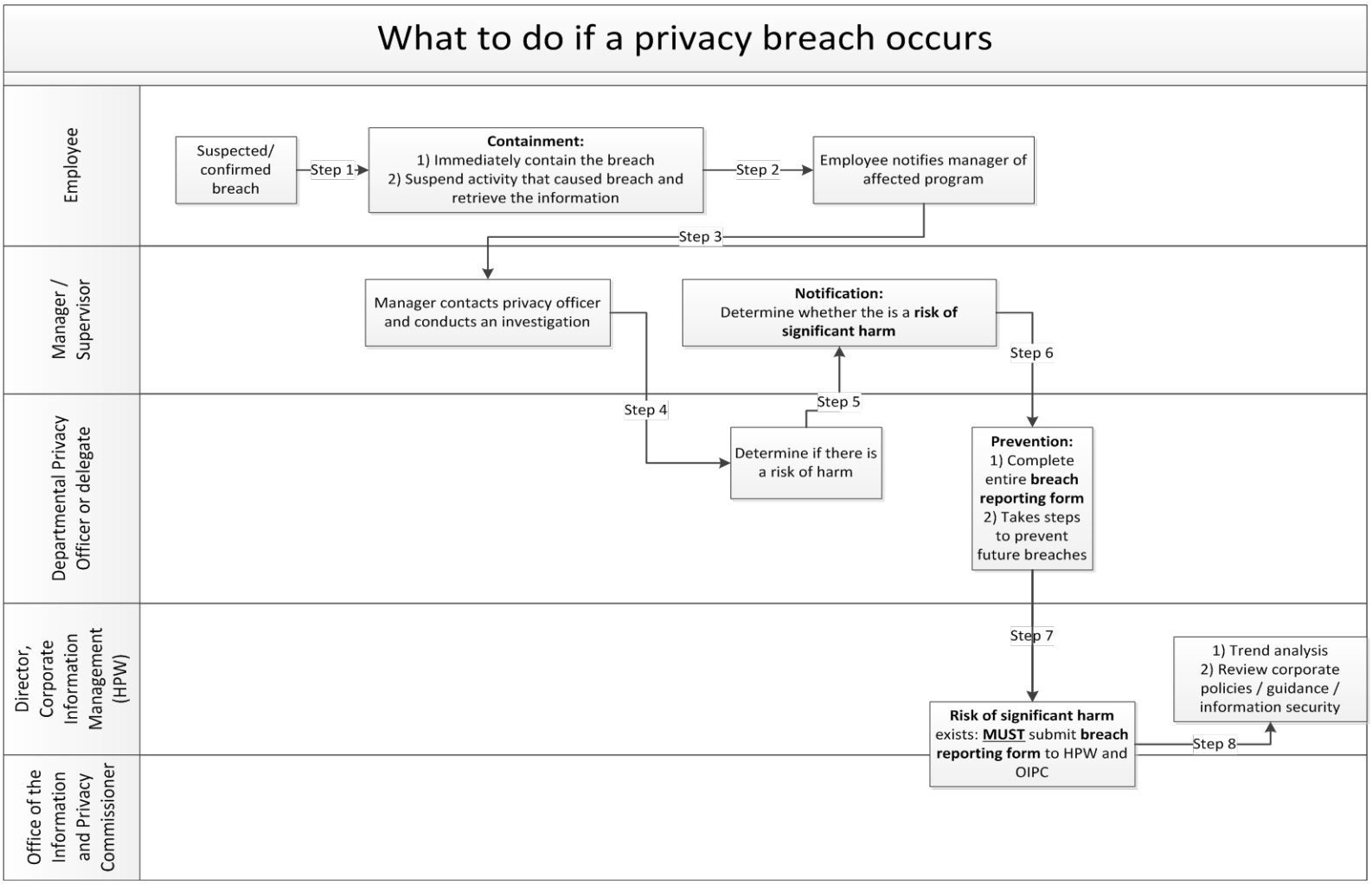
Control – Individuals have a right to know about matters relating to how their information has been accessed, used or disclosed, including inadvertent access or loss of their information.

Trust – The public's expectation that the government will be upfront and honest with individuals about how their information has been accessed, used or disclosed.

Transparency – The obligation to communicate and be transparent with individuals about how their information has been accessed, used or disclosed.

What do I do if a privacy breach is suspected or has occurred?

Steps involved in responding to a privacy breach are detailed in the flowchart below.


What to do if a privacy breach occurs
Employee
Manager / Supervisor
Departmental Privacy Officer or delegate
Director, Corporate Information Management (HPW)
Office of the Information and Privacy Commissioner
Suspected/ confirmed breach
Step 1
Containment:
1) Immediately contain the breach
2) Suspend activity that caused breach and retrieve the information
Step 2
Employee notifies manager of affected program
Step 3
Manager contacts privacy officer and conducts an investigation
Notification:
Determine whether the is a risk of significant harm
Step 6
Step 4
Step 5
Determine if there is a risk of harm
Prevention:
1) Complete entire breach reporting form
2) Takes steps to prevent future breaches
Step 7
1) Trend analysis
2) Review corporate policies / guidance / information security
Risk of significant harm exists: MUST submit breach reporting form to HPW and OIPC
Step 8

Step 1: Employee or program manager contains the breach

Recommended timeline: Within one hour

- Call your IT representative if the breach relates to unauthorized access to a digital information system.
- If you're uncertain whether a breach occurred, immediately contact your departmental privacy officer for confirmation.

Step 2: Employee notifies supervisor or program manager

Recommended timeline: Immediately

- If the manager or supervisor believes the breach resulted from criminal activity, notify the RCMP immediately.
- The manager or supervisor should notify the affected program's Director.

Step 3: Program manager notifies departmental privacy officer

Recommended timeline: Same day the breach is discovered.

- After notifying the departmental privacy officer, the program manager or supervisor can download the *Privacy Breach Reporting Form* and answer questions 1.1 and 1.2.
- In collaboration with the Manager or Supervisor, the privacy officer will determine among the department's senior management should be notified. For example, Director of Communications, ADM, and/or DM.
- The privacy officer will determine whether the breach involves other departments.
- The privacy officer determines who will be the lead in completing the *Privacy Breach Reporting Form* and reporting back to the program manager, privacy and, if needed, senior management.

Step 4: Privacy Officer or delegate determines the risk of harm to affected individual(s)

Recommended timeline: Within 5 working days after breach was discovered or reported.

- Privacy officer or delegate completes section 2 of the *Privacy Breach Reporting Form.*
    - The privacy officer may also create a breach response team. A breach response team may include representatives from: legal services branch, the ATIPP office, IT unit, IM unit, and individuals from the affected program.

Step 5: Program manager notifies affected individual(s), if needed

Recommended timeline: Within 2 – 3 weeks after breach was discovered

- The privacy officer or delegate will determine whether notification is required or appropriate. Use the parameters set forth in question 2.4 when making this determination.
- **When there is a risk of significant harm:**
    - If there is a risk of significant harm, affected individuals **MUST** be notified.
    - In addition, the Office of the Information and Privacy Commissioner (OIPC) must at the same time be given notice. Be mindful not to identify affected individuals when notifying the OIPC.

- **When there is not a risk of significant harm:**
    - If it is determined that there is not a risk of significant harm, departments are not obliged to notify affected individuals or the OIPC. However, this is not to say that departments should not notify. Use the guiding principles to assist in determining whether or not to notify those affected by the breach or the OIPC.
- **Notification process.**
    - *When:* If notification is to take place, it should occur as soon as possible. However, if you have contacted the RCMP, you should confirm whether notification will impede their investigation.
    - *How:* Notification should be direct (that is, by phone, letter or in person). Indirect notification (that is, website information, posted notices, media) should occur only where direct notification could cause further harm, is cost prohibitive and/or there is insufficient contact information available. The tables below set out factors to consider when deciding how to notify affected individuals.

Considerations Favouring DIRECT Notification
✓ The identities of the affected individuals are known
✓ Current contact information for the affected individuals is available or can be obtained
✓ Whether affected individuals require detailed information in order to properly protect themselves from harm resulting from the breach
✓ *Whether* affected individuals may have difficulty understanding an indirect notification (due to mental capacity, age, language, …)

Considerations Favouring INDIRECT Notification
✓ *Direct notification is impracticable because t*he number of affected individuals is large, or their contact information is unavailable
✓ Direct notification could compound the harm to the individual resulting from the breach

    - *What to include in the notification:* The purpose of notifying individuals is to reduce or prevent harm that could be caused by the breach. The *Privacy Breach Reporting Form* establishes the minimum requirements when notifying affected individuals (see question 3.2). As a best practice, your notice should include the information below:

Information Required in the Notification
✓ Date of the breach
✓ General description of the breach
✓ Description of the information / provide an overview of the type of information involved in the breach *The information should be general and should <u>NOT</u> include any personal information involved in the breach. For example, you can say that the individual's date of birth was involved, but you would not state the individual's actual date of birth in the notification.*
✓ Steps taken so far to control or reduce the harm

✓ Future steps planned to prevent further privacy breaches
✓ Steps the individual can take: *Provide information detailing how individuals can protect themselves in light of the breach. For example, to contact credit reporting agencies to set up a credit watch or explain how to change a personal health number or drivers licence number. In certain circumstances it may be appropriate to pay for credit monitoring of affected individuals.*
✓ Contact information of an employee for further assistance: *Provide contact information for someone within your organisation who can answer questions, provide addition information and offer assistance to affected individuals.*
✓ Office of the Information and Privacy Commissioner's contact information *Provide OIPC contact information and notify individuals of their right to make a complaint to the OIPC.*

Step 6: Privacy Officer or delegate prevents future or similar breaches

Recommended timeline: Within 4 – 6 weeks after the discovery of the breach

- The privacy officer or delegate will complete the entire *Privacy Breach Reporting Form.*
- Things to consider when formulating internal improvements:
    - Thoroughly examine and understand the cause of the breach. Be certain whether the cause was a failed physical, technical or administrative safeguard. For example, if the breach resulted from weak administrative safeguards and mitigation strategies only focused on physical safeguards, you will not have prevented future breaches from occurring. In some cases, a security audit may be necessary.
    - Develop or improve, as necessary, adequate long-term safeguards against further breaches.
    - Review policies and update them to reflect lessons learned from the investigation.
    - Audit at the end of the process to ensure that the prevention strategy has been fully implement.
    - Associate timelines with prevention strategy.
    - Review, update and provide privacy training.

Step 7: Privacy Officer or delegate submits completed privacy breach reporting to OIPC and HPW

Recommended timeline: Within 1 – 2 weeks after completing the entire *Privacy Breach Reporting Form*

- **When there is a risk of significant harm.**
    - Submit the *Privacy Breach Reporting Form* to both the OIPC and the Director, Corporate Information Management at HPW within a reasonable amount of time after notifying the affected individuals.
    - The requirements for reporting to the OIPC are found in:
        - Health Information Privacy and Management Act, section 31(1), if your breach involves personal health information.

        - Privacy Breach Policy (created under the authority of GAM 2.27), if your breach involves personal information.
    - The reporting requirements to the Director, Corporate Information Management, are found in:
        - Privacy Breach Policy, for breaches involving either personal information or personal health information.

- **When there is no risk of significant harm:**
    - If it is determined that there is not a risk of significant harm, departments may submit the *Privacy Breach Reporting Form* to the OIPC or the Director, Corporate Information Management. There are benefits in voluntarily contacting these offices.
        - Contacting the OIPC: This office has a lot of expertise around the management of both personal information and personal health information. Staff can assist in improving programs' controls to mitigate a similar breach from reoccurring.
        - Contacting the Director, Corporate Information Management: The Director can offer assistance and resources to help respond to breaches, including improving program controls. In addition, you can contribute to preventing similar occurrences from happening elsewhere in Yukon government by improving corporate knowledge and understanding of how sensitive information is managed.

          Note: You do not have to identify the program or employees involved in the breach. The discussion is about the <u>incident</u> and preventing future breaches from occurring in other programs across Yukon government by sharing lessons learned.