Privacy Breach Procedures:
Compliance for written practice for privacy breaches

Purpose and Intended Audience:

This resource responds to the need to establish an administrative security measure (written practice) prescribed by section 9(3)(a) of the *ATIPP Regulation*.

The target audience are Designated Privacy Officers (DPOs) because they will be controlling the process.

It provides an overview of specific responsibilities, processes and timing involved for what is required for an "employee" to report unauthorized use, disclosure and suspected privacy breaches. See the *ATIPP Act* for the definition of "employee" of a public body.

It also outlines the specific responsibilities, processes and timing involved for DPOs and Heads of public bodies to respond to, assess, and report on breaches.

For a more detailed description of the functions and activities assigned to DPOs, as well as more information about privacy breaches, please check out the Designated Privacy Officer Toolkit.

The timelines associated with breach reporting is an important piece that is not included in the *ATIPP Act/Regulation* and this guidance is intended to address these timelines.

Context from the *ATIPP Act/Regulations*

Section 30 of the *ATIPP Act* states:

"**Securing personal information against privacy breach**

30 The head of a public body must protect personal information held by the public body by securely managing the personal information in accordance with the regulations."

And, according to the *ATIPP Regulations*, secure management of personal information and security measures must include:

"9(3)(a) **a written practice respecting privacy breaches** that sets out the responsibilities of **employees under sections 20, 24 and 31** of the Act and of **designated privacy officers and heads of public bodies under section 32** of the Act"

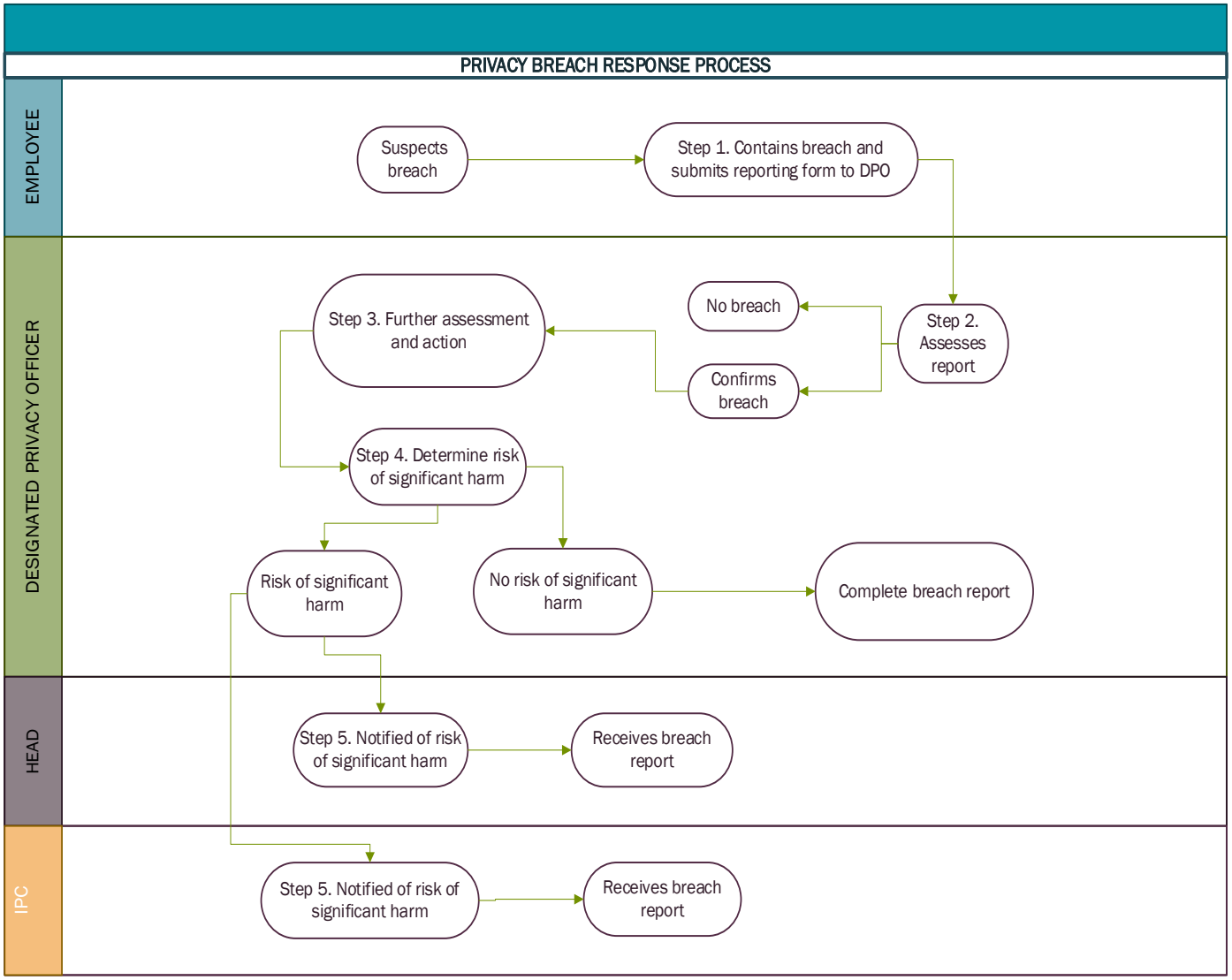
A ***written practice*** that sets out responsibilities of employees includes:

- Employee to **report suspected unauthorized use** (ATIPP Act, section 20)
- Employee to **report suspected unauthorized disclosure** (ATIPP Act, section 24)

- Employee to **report suspected privacy breach** (ATIPP Act, section 31)
- A written practice that sets out responsibilities of DPOs and heads includes:

Response to **report of suspected privacy breach** (ATIPP Act, section 32)

Steps involved in the privacy breach response process:



*** <u>AFFECTED INDIVIDUALS MUST BE NOTIFIED WHEN THERE IS A RISK OF SIGNIFICANT HARM</u> ***

***** The Access and Privacy Officer must receive a copy of the breach report when risk of significant harm to individuals is present and the breach involves a **Ministerial public body.**

Step 1. Employee contains the breach and submits reporting form to Designated Privacy Officer

Timeline: Immediately

- Complete the 'Privacy Breach Reporting Form for Employees' and submit it to the public body's Designated Privacy Officer (DPO)
- Call IT representative if the breach relates to unauthorized access to a digital system.
- If uncertain whether a breach occurred, immediately contact the DPO for confirmation.

Step 2. DPO assesses report to determine if breach has occurred

Recommended timeline: Same day as the breach is reported

- Discuss the suspected breach with the employee to gather facts and additional information if needed.
- Determine whether the suspected breach involves one or multiple departments.
- Evaluate the suspected breach by reviewing the incident with the public body's governing legislation, as well as any existing agreements, policies, protocols and privacy compliance documents.

Step 3. Further assessment and action

Recommended timeline: Immediately

- Notify the affected program's director and in collaboration with the director, determine who among the department's senior management should be notified.
- Determine whether the breach involves other public bodies and notify other Designated Privacy Officers as required.

Please note: Section 32(4) of the ATIPP Act states that *without delay* after receiving a request from the DPO for the purposes of a breach assessment, the head or employee who received the request must, if they hold the information requested, provide it to the Designated Privacy Officer.

Step 4. Determine Risk of Significant Harm

Recommended Timeline: 5 working days after discovery of the breach

To determine whether there is a risk of significant harm, the DPO must first determine the significant harm associated with the breach. A factor in this determination is the sensitivity of the information involved in the breach.

Significant harm includes bodily harm, humiliation, damage to reputation or relationships, loss of employment, business or professional opportunities, financial loss, identity theft, negative effects on their credit record, and damage to or loss of property.

Next, the DPO must determine if there is a risk, meaning "possibility" that the individual may suffer or be exposed to the significant harm. The DPO should consider the factors outlined in paragraphs 32(6)(a) through (h) of the *ATIPP Act* to make this determination.

Risk of significant harm can be determined by considering these factors:

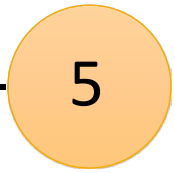
- The sensitivity of the personal information (PI) involved;
- The probability that the PI is, has been, or will be used or disclosed in an unauthorized manner;
- How much time passed from the occurrence of the privacy breach and its discovery;
- The number of affected individuals;
- The type of relationship, if any, between affected individuals and any person who may have seen the PI (this is a factor of particular importance in a small jurisdiction such as the Yukon);
- The measures, if any, that the public body has implemented or is implementing to reduce the risk of significant harm to the affected individuals;
- If the personal information has been lost, stolen or disposed of, whether or not any of it has been recovered;
- The possibility/likelihood that the information could be used for identity theft or fraud;
- How many people had access to the PI;

- Immediate containment and mitigation measures able to taken; and
- Any other available information that is relevant in the circumstances.

If risk of significant harm is identified for one or more individuals, continue on to Step 5 – Notification. This information – risk of significant harm analysis – is documented in Section 3 of the Designated Privacy Officer Breach Reporting Form.

If the outcome of the analysis reveals no risk of significant harm to affected individual(s), continue to Step 6 - Complete DPO Breach Reporting Form section.

Step 5. Notification



Recommended Timeline: within 2 – 3 weeks after discovery of the breach

- If there is a risk of significant harm, all affected individuals MUST be notified.
- Risk of significant harm also triggers notification to applicable Head(s), and to the Office of the Information and Privacy Commissioner (OIPC)
- This means that notifications should be instigated prior to fully completing the breach report. After notifications are accomplished, circle back to completing the form.
- Direct notification to affected individuals is required unless one of the circumstances in Section 10 of the ATIPP Regulations is present. Section 10 of the ATIPP Regulations prescribes the circumstances under which public notices may be provided rather than notifying individuals directly. The OIPC must be notified at least one day in advance of a public notice.
- Both direct and public notices to individuals affected by risk of significant harm must contain certain information as prescribed by the ATIPP Regulations. See Section 10 (7) of the ATIPP Regulation. There are also requirements for what should be included in a notice to the OIPC.
- Use the Privacy Breach Notification Template provided by the ATIPP Office.

Step 6. Complete Designated Privacy Officer Breach Reporting Form

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

- Complete the Designated Privacy Officer Breach Reporting Form issued by the ATIPP Office.
- Thoroughly examine and understand the cause of the breach. Be certain whether the cause was a failed physical, technical or administrative safeguard. 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.
- Audit at the end of the process to ensure that the prevention strategy has been fully implemented.
- Provide the Office of the Information and Privacy Commissioner (OIPC) with a copy of the breach report if the breach involves a risk of significant harm to affected individual(s).
- The Head of the public body has 30 days after which receiving any recommendations from the OIPC to respond and provide a notice of their decision relating to any recommendations.

Step 7. Manage Designated Privacy Officer Breach Reporting Form

- Breach Reports should be filed according to 0252-04 in the Administrative Records Classification System (ARCSv.3). This records retention and disposition schedule (ARCSv.3) allows for the destruction of breach reports 3 years after the closure of the file, which happens at the end of the fiscal year in which the reports are written. Contact your Department's Designated Records Officer for more information.
- Record information for statistical purposes about the breach on the Privacy Breach Reporting status page on the Privacy Management SharePoint site. Information documented on this page includes (by public body): number of privacy breaches and number of privacy breaches that include risk of significant harm to affected individuals per fiscal year.