Fact Sheet: Privacy Incident Response

The *Protection of Privacy Act* (POPA) establishes requirements for the protection of personal information, data derived from personal information and non-personal data against such risks as unauthorized access, collection, use, disclosure or destruction.

Protection of Privacy

All public bodies are responsible for safeguarding the information in their custody or under their control. Specifically, public bodies are required to protect:

- Personal information in the custody or under the control of the public body (section 10(1)),
- Data derived from personal information created under section 17(1) (section 20), and
- Non-personal data created under section 21(1) (section 24).

This protection is achieved by requirements for public bodies to implement reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or destruction. When information is not adequately protected, privacy incidents may result.

While the head of the public body holds primary accountability for compliance with these requirements, the obligation to protect information extends to all employees of the public body.

Employees are defined under the Act (section 1(h) and include a person who performs a service for the public body as an appointee, volunteer or student or under a contract or agency relationship with the public body.

Privacy Incidents

A privacy incident, as described in section 10(2) of POPA, occurs when personal information – or data derived from personal information – under the custody or control of a public body is lost, accessed or disclosed without authorization, and there is a real risk of significant harm (RROSH) to an individual as a result.

As data derived from personal information can still identify individuals (section 1(e)), a loss, unauthorized access, or unauthorized disclosure also qualifies as a privacy incident under section 10(2). For more information, refer to the Fact Sheet: Data Matching and Data Derived from Personal Information or the *Protection of Privacy Act* Guide.

Privacy incidents may result in significant harm to individuals, but also to organizations, and public bodies. Therefore, taking appropriate steps to contain an incident with an efficient and coordinated approach, minimizes the harm that it may cause to all parties, especially individuals.

A public body's response to a privacy incident should reflect the security classification of the information including the notification process. If an incident occurs as described in section 10(2), POPA requires a public body to complete notification. For more information, refer to the Fact Sheet: Privacy Incident Notification.

Not all incidents will meet the threshold for mandatory notification under RROSH. However, it is essential that public bodies consistently track, assess, and respond to all privacy incidents - regardless of whether notification is required - and take steps to prevent recurrence. Doing so helps public bodies ensure they are meeting their obligations to protect personal information in their custody and control in all instances.

The steps listed below may help public bodies assess and respond to incidents, mitigate harm, and implement measures to prevent recurrence.

Incident Response Steps

Six key steps are recommended for responding to a privacy incident; however, they are not exhaustive. Public bodies must evaluate each incident individually and determine whether additional actions are required.

The six steps are:

1. Containment
2. Initial Reporting
3. Investigation and Evaluation of Risk
4. Notification
5. Additional Measures
6. Prevention

Note: Steps 1 and 2 may be completed simultaneously or in quick succession immediately following the incident.

Step 1: Containment

As soon as an incident is identified, limiting the extent and impact of the incident is a priority.

1. Public body employees should notify their supervisor and take necessary actions to immediately contain and document the details of the incident.
    a. Examples of common privacy incidents and recommended containment best practices are provided at the end of this procedure.
2. Other areas within the public body that need to be involved to immediately contain the incident should be identified and contacted (e.g., system administrators, relevant security teams, etc. See Step 2 for more information).

Step 2: Initial Reporting

Prompt reporting of a privacy incident is essential to ensure timely containment and initiate a thorough investigation.

1. Report the incident to your public body's designated Privacy Officer, or Privacy Office, and/or legal counsel, as per your internal incident reporting process (see the Privacy Management Programs section), providing any necessary and relevant details.
    a. If there is uncertainty whether a situation constitutes a privacy incident, it is recommended that it be reported to your Privacy Officer/Office, and/or legal counsel, to assist in the determination.
2. Contact the appropriate team (for example: cybersecurity, information technology (IT), systems people etc.) within your public body immediately if the incident involves an IT system/device/application that is suspected to be or has been compromised.
3. If the privacy incident involves suspected theft or criminal activity, contact the appropriate police agency.

If there is uncertainty with regard to the parties that need to be contacted, contact your Privacy Officer/Office for assistance.

Step 3: Investigation and Evaluation of Risk

During their investigation, in conjunction with the public body, the designated Privacy Officer/Office, and/or legal counsel, should:

- Gather all relevant information to determine the nature and extent of the incident,
- Evaluate whether the incident meets the threshold for RROSH, preparing an analysis of the harm assessment, and
- Provide the public body with recommendations on next steps, including, but not limited to, notification, additional mitigation measures, and preventative measures to prevent reoccurrence of future incidents.

To determine whether an incident meets the threshold for RROSH as described in section 10(2) of POPA, the Protection of Privacy (Ministerial) Regulation identifies the factors constituting "real risk of significant harm" in section 4(1) and what would be considered "significant harm" in section 4(2).

If any other relevant factors exist not included in the regulation, they should also be considered during the public body's assessment. These may include, but are not limited to:

- The number and type of individuals impacted by the incident (e.g., employees, clients, contractors, etc.).
- The safeguards in place at the time the incident occurred (e.g., encryption, limitations on access, physical storage, etc.).
- The type of unauthorized recipient, and the type of relationship between them and the impacted individual(s), if any (e.g., incorrect client from the same program, unauthorized employee, member of the public, etc.).

Alberta's Information and Privacy Commissioner's website and office has resources available to help determine risk and can also provide advice on a case-by-case basis if RROSH may apply.

Step 4: Notification

The outcome of the investigation and harm assessment in Step 3 determines whether notification is mandatory under POPA.

If the incident meets the threshold for RROSH:

As described in section 10(2), if, based on the risk of harm assessment, it is determined that the incident meets the threshold for RROSH, the public body is required to give notice to the impacted individual(s), Alberta's Information and Privacy Commissioner, and the Minister responsible for this Act (the Minister of Technology and Innovation). This also applies if the incident involves data derived from personal information.

Public bodies must give written notice through one of the authorized methods listed in section 53 of POPA; the notice must comply with the prescribed requirements set out in sections 4(3) to 4(5) of the Protection of Privacy (Ministerial) Regulation, as per section 10(3) and must be completed without unreasonable delay. For information on notification requirements, refer to the Fact Sheet: Privacy Incident Notification.

Notification should not occur prior to consulting with your Privacy Officer/Office, and/or legal counsel. They may assist by providing notification template(s), if available, or provide instructions on how to complete and submit notice to the necessary parties.

If the incident does **not** meet the threshold for RROSH:

In the case that an incident does not meet the threshold for RROSH, public bodies may still choose to notify the impacted individual(s) as a best practice measure, promoting transparency, accountability, and further minimizing the harm that an incident may cause.

Public bodies are not required to notify the Information and Privacy Commissioner nor the Minister in these cases, however, they may voluntarily report to the Commissioner if they wish. Whether or not the public body chooses to notify, it is recommended that they still document all incidents for the purposes stated in Step 6.

If a public body chooses to voluntarily notify the impacted individual(s) and/or the Commissioner, they are encouraged to align their notices with the respective requirements for these two parties - sections 4(3) and 4(4) of the Protection of Privacy (Ministerial) Regulation and follow the notification requirements under section 53 of POPA. Refer to your Privacy Officer/Office, and/or legal counsel, for assistance and the Fact Sheet: Privacy Incident Notification for more information.

Step 5: Additional Measures

Depending on the circumstances of the incident, your Privacy Officer/Office, and/or legal counsel, may recommend additional mitigation measures. For example, offering to provide credit monitoring to the impacted individual(s) if the incident involved their social insurance number, or other financial information.

The circumstances of each incident vary. Similarly, the appropriate mitigation measures, or whether other steps are needed equally vary. Public bodies, together with their Privacy Officer/Office, and/or their legal counsel, should exercise their judgement on each incident and consider what other steps may be necessary, if any.

Step 6: Prevention

Following the completion of the investigation, public bodies should evaluate and set up appropriate prevention measures to minimize the risk of similar privacy incidents from occurring, based on the evaluation from Step 3 and recommendations from your public body's Privacy Officer/Office, and/or legal counsel. This may include updating policies or procedures, improving security safeguards, or providing additional training to staff on privacy practices. Where applicable, other relevant groups that were reported to in Step 1 or Step 2, may provide additional recommendations.

As with the mitigation measures, the appropriate preventative measures are dependent on the circumstances of the incident. Public bodies should again, together with their Privacy Officer/Office, and/or legal counsel, exercise their judgement on each incident and consider what other measures may be necessary, if any.

Finally, it is recommended that public bodies keep a record of **all** privacy incidents in their public body as reference to investigate potential trends and determine areas of improvement.

Privacy Management Programs

As part of the privacy management program (PMP) requirements under section 6(1)(b)(i)(B) of the Protection of Privacy (Ministerial) Regulation, all public bodies are required to establish internal policies and procedures for handling incidents as described in 10(2) of the POPA.

It is the responsibility of each public body to ensure that all employees – including contractors – are informed of, and understand these policies and procedures, as well as their specific responsibilities related to privacy incident management and notification. For example, notifying their supervisor and other parties as required when an incident is first discovered. For more information, refer to the Fact Sheet: Privacy Incident Notification and the Fact Sheet: Privacy Management Programs.

Refer to your internal policies and procedures for more information on how your public body handles these incidents and notification.

Role of the Privacy Officer/Office

As required under section 6(1)(a) of the Protection of Privacy (Ministerial) Regulation, all public bodies must designate or identify a Privacy Officer.

This Privacy Officer is the designated employee responsible for the public body's compliance with the Act. Various aspects of this Privacy Officer's position may vary depending on the size of the public body, the delegated authorities, and the volume and sensitivity of information handled by the public body.

However, in regard to privacy incidents, their responsibilities include:

- Leading investigations into privacy incidents and assessing the associated level of harm.
- Providing recommendations to ensure compliance with POPA and prevent reoccurrence of incidents.
- Overseeing day-to-day operations of POPA within the public body.

Some of these responsibilities, including leading investigations into privacy incidents, may be assigned to other individuals, such as a public body's legal counsel, or other employee based on the public body's delegated authorities. Refer to your internal policies and procedures for more information.

Depending on the size of the public body, some may have a full time Privacy Officer with additional staff in a Privacy Office, while others may have an officer that only works in that capacity on an "as needed" basis. Regardless of structure, the Privacy Officer or Office should be the focal point for protection of privacy expertise within the public body.

Examples of Common Privacy Incidents and Potential Containment Actions

Potential Incident	Potential Containment Actions
Misdirected email to wrong client/public body employee or other unintended recipient.	• Request an email recall through your email system, if function is available. • Where a group email includes an untended recipient remove unintended recipient, resend email requesting staff to delete and not respond to the original email. • Contact unintended recipient, advising information was sent in error and request them to double delete the email from both their inbox and deleted box. Confirm information was not read and no copies were made.
Documents are mailed or sent to the wrong individual.	• Contact unintended recipient and request the records be returned or destroyed.
Public body employee uploads documents for one client into another client's file.	• Restrict access or delete the information from the uploaded information. • Review to ensure correct personal information is places on the right file. • Contact the unintended recipient and request them to delete it on their side (if possible). • Confirm no copies of the information were made or retained.
A public body employee's work laptop and/or cellphone is stolen.	• Contact appropriate team (for example cybersecurity, information technology, etc.) to request device be remotely wiped and request them to confirm if any attempts at log-in were received after last known employee's use. • Contact law enforcement to report theft.
A public body employee accessed third party personal information (such as family members, friends, neighbors etc.) on a public body's database or file system.	• Restrict access to the files. • Restrict access for the public body employee to any information.
Potential inadvertent destruction of personal information records.	• Confirm and investigate missing records. • Determine if the missing records were inadvertently destroyed.