Managing a Privacy Breach

Protocol and Forms

Information Access and Privacy (IAP) Services
Information, Communications and Technology Services
Department of Internal Services

July 2017
Version 1.0

NOVA SCOTIA

Contents

Introduction

Every public body that collects, uses or discloses personal information is responsible for ensuring it is secure and handled appropriately. Information Access and Privacy (IAP) Services has created this privacy breach protocol to follow, should a privacy breach occur. This protocol is a companion document to the corporate Privacy Policy and will guide the decision making and documentation that is required in response to a privacy breach.

As a reminder, personal information is defined in the Freedom of Information and Protection of Privacy (FOIPOP) Act and includes:

(i) the individual’s name, address or telephone number,
(ii) the individual’s race, national or ethnic origin, colour, or religious or political beliefs or associations,
(iii) the individual’s age, sex, sexual orientation, marital status or family status,
(iv) an identifying number, symbol or other particular assigned to the individual,
(v) the individual’s fingerprints, blood type or inheritable characteristics,
(vi) information about the individual’s health-care history, including a physical or mental disability,
(vii) information about the individual’s educational, financial, criminal or employment history,
(viii) anyone else’s opinions about the individual, and
(ix) the individual’s personal views or opinions, except if they are about someone else;

What is a Privacy Breach?

As defined in the Privacy Policy, a privacy breach occurs when there is the intentional or unintentional unauthorized collection, use, disclosure, disposal, modification, reproduction, access or storage of personal information, that is in violation of the Freedom of Information and Protection of Privacy (FOIPOP) Act or the Personal Information International Disclosure (PIIDPA) Act.

Some common types of breaches are:

- Sending documents containing personal information in any way to the wrong person. For example, sending an email to the wrong address.
- Snooping through files or database systems looking at personal information that you have no need to know.
- Discussing someone else’s personal information with any person, whether inside or outside the workplace, who does not have a need to know that information
- Testing computer systems using actual personal information as opposed to dummy data or using information that has identifiers removed.
- Sharing your password to a system.
- Data entry error or perhaps a technical error that results in someone getting someone else’s information, such as on a permit or licence

- Disclosing personal information of a client(s) to the public with malicious intent, this would include posting online such as through social media.

In some instances, the following events could result in a privacy breach:

- Theft or loss of equipment or devices containing personal information.
- Carelessness in the transporting or handling of electronic devices such as memory sticks, laptops or tablets outside of the office without adequate security measures.
- The sale or disposal of equipment or devices containing personal information without proper disposal procedures being carried out prior to the disposal or sale.
- Unlocked office doors or filing cabinets or computers that are not logged off.
- Breach of the network security that allows for a hacker to gain access to personal information.
- Not ensuring that you verify the person’s identity before disclosing personal information.
- Not disposing of documents or portable storage devices in a secure manner, such as shredding documents or wiping a device.
- Not storing information in a secure manner, such as not using encryption or controlling access to shared folders.

Privacy incidents are a subset of privacy breaches. Incidents are typically less severe than a privacy breach. An incident occurs when personal information is mishandled or incorrectly collected, used or disclosed in a limited or controlled environment. In these instances, the situation can be easily and quickly corrected without any harm to the individual. They are usually resolved immediately by the employees who become aware of them but if not addressed can escalate into a full-scale breach. Examples of incidents and options to address them include:

- Inadvertent storage of personal information – that can be resolved by properly filing a misfiled record
- Data entry error of personal information – that is corrected before being used for decision making

All known or suspected breaches or incidents require immediate remedial action, no matter the type or information or the perceived sensitivity of the personal information. Given the varied nature of privacy breaches, there is never a one-size-fits all response. All actions taken should be proportionate and appropriate to each breach.

This protocol will help to make that determination as well as providing guidance through completion of the four essential steps of a breach response. This protocol should be followed whether the breach has occurred internally or a third-party service provider notifies that they have discovered a breach that affects personal information entrusted to them, yet still under the public body’s control.

Breach Management Process

If a breach has been identified, then you must act immediately to:

1. contain the breach
2. evaluate the breach and assess the risk
3. notify and report details of the breach
4. investigate the cause to prevent future breaches

The first three steps must be completed as soon as possible following a breach and will most likely be done simultaneously. The fourth step addresses longer-term solutions and prevention strategies.

Documentation of the resolution of the breach at all stages must be kept. The response to the breach must be documented using the **Privacy Breach Report** form in Appendix A. (Word versions of all forms are available on the IAP Services website)

Roles and Responsibilities

Responding to a privacy breach may require the involvement of many individuals, each will have a specific role in the process and many will form part of the breach response team.

Employee	• Identifies possible privacy breach • Immediately reports suspected breach to their supervisor • Undertakes or assists with containment efforts • Assists with breach investigation as required
Supervisor	• Immediately reports suspected breach to the Privacy Designate/IAP Administrator • Immediately undertakes containment efforts • Completes breach report or ensures it is completed • Assists with breach investigations as required
Privacy Designate/IAP Administrator	• Receives notification of possible breach • Assesses and confirms if a privacy breach occurred • Co-leads the breach investigation • Conducts an assessment on the breach to determine level of risk • Recommends containment efforts • Determines who needs to be notified internally in consultation with the supervisor • Supports the program/business area leadership to establish a breach response team if required • With breach response team, determines if external notifications are required • Works with Communications and the program/business area to ensure notification is made to the affected individuals, including review of scripts, letters etc. • With the breach response team, identifies risk mitigation and prevention strategies

Program/Business Area Leadership	- Leads the breach response team - Identifies containment, mitigation and prevention strategies - Undertakes containment efforts - Co-leads the breach investigations - Completes or assists with completing breach report - Actions recommended risk mitigation and prevention strategies
IT resources/Cybersecurity	- Participates on breach response team where the breach involves IT resources - Facilitates containment, mitigation and prevention strategies especially as they relate to system-related breaches
Legal counsel	- May participate on the breach response team If legal action is possible or legal interpretation is required - May assist in determining if external notification is required
Communications Director	- May participate on the breach response team - Assist in developing communications for external notification of affected individuals, when required - Prepares public messaging if necessary
Human Resources	- Participates on breach response team where personnel issues are involved (e.g., in cases of employee snooping) - Responsible for notification to the union if necessary
Deputy Head/ Other Executive Leadership	- Receives notifications and reports from breach response team - Signs off final report
Privacy Program, Information Access and Privacy Services	- Receives a report on all breaches - Provides advice on containment, mitigation and prevention strategies - May form part of the breach response team where required - Provides guidance on determining if notification to the Office of the Information and Privacy Commissioner (OIPC) is necessary - Coordinates communication and processes with the Commissioner's office.
Chief Information Access and Privacy Officer	- Receives notifications and reports from breach response team - May form part of the breach response team when required - Makes final decision regarding external notification and notification to the OIPC

The above table lists the main roles that will be involved in responding to a breach. There may be other individuals who may need to participate in the process, depending on the nature of the breach. These may include security/facility management, insurance and risk management or third-party service provider representatives. There may also be external parties that need to be engaged such as the police, professional or other regulatory bodies, financial institutions or credit reporting agencies. Determining when these roles or organizations may need to be engaged will occur as the investigation into the breach evolves and the breach response team has enough information to make recommendations.

Responding to a Privacy Breach

Step 1: Contain the Privacy Breach

Initiate this series of steps as soon as a privacy breach is thought to have occurred or is discovered. These steps should be completed in very quick succession.

1.1 Notify Supervisor

An employee who identifies that a possible privacy breach has occurred, should immediately notify their supervisor.

1.2 Notify Privacy Designate or IAP Administrator

The supervisor should immediately contact the privacy designate/IAP administrator who will provide guidance on this protocol. The privacy designate/IAP administrator will assist in assessing the situation and determining next steps. This initial assessment will focus on answering the following questions:

- Did an inappropriate collection, use or disclosure of personal information occur?
- Does personal information continue to be at risk?
- Do clients or employees continue to be concerned?
- Is there a possible violation of policy or law?

The answers to these questions will determine whether a privacy breach or privacy incident has occurred. It is possible that what happened was not a privacy breach but was a privacy incident.

1.3 Contain the Breach

In conjunction with the supervisor, the employee should begin to immediately contain the breach. Steps should be taken to prevent any further disclosure of the personal information and/or secure and recover any personal information that has been disclosed. The steps will vary depending on how the breach occurred.

Actions that should be taken to contain a breach are:

- If something was sent to the wrong mailing address or fax number, contact the recipient and ask them to return the records and confirm that no copies were made, in writing if possible. If feasible retrieve the records in person.
- For a misdirected email, if you can, try to retract the email or contact the recipient and ask them to delete the email from their system and confirm that there was no further disclosure of the email
- If a document, file, portable storage device, was misplaced, attempt to locate.
- For lost or stolen electronic devices (mobile phone, laptop or tablet), contact the Service Desk to report the device was lost or stolen so that a signal can be sent to attempt to locate and/or wipe the device.
- If a system appears to be compromised, immediately contact the Service Desk to discuss taking the system off-line until further investigation can take place to fix security risks/weaknesses.
- If a user-id or password to a system has been compromised, immediately change the password.

1.4 Establish Response Team

Depending on the nature of the breach, the supervisor, program/business area leadership and privacy designate/IAP administrator should action an escalation protocol. This protocol will identify who within the organization needs to be notified that a breach occurred. Who is notified at this point is based on the initial information about the breach. This notification may include senior management, deputy head, and communications.

Many of the individuals notified also need to work together to respond to the breach. This is the breach response team. This is where the previously identified roles come into play. It is within this team where decisions will be made to determine what other notifications will be necessary (i.e. police, HR or legal counsel).

Step 2: Assess the Extent and Impact

Evaluating potential risks to affected individuals is key in responding to the breach. It is critical to understand the scope of the breach, who is affected and how they may be affected.

The **Privacy Considerations Table** in Appendix B along with a preliminary breach report should be used to record information about all the factors that need to be considered in this next series of steps. The answers to the questions are critical in fully understanding all that is involved in the breach, including the cause and extent and importantly how those impacted could be harmed.

2.1 Assess the Personal Information Involved

- Identify what type of personal information was breached.
- Once information that is part of the breach is known, assess it for risk level based on what type of personal information it is. Personal information is not all equally sensitive, and should be assessed on a case-by-case basis. Government issued or stored information like SIN cards, financial information, driver's license, health information is usually considered sensitive. Often a combination of personal information is more sensitive than any single piece.
- Context is also important to consider when evaluating a breach. If personal information is leaked but not associated with names, the sensitivity would be far less than identifiable information. Likewise, a generic list of people who have accessed government services in the last year will be less sensitive than a list of people and the specific government service they have used.

2.2 Cause and Extent of the Breach

To understand the cause and extent of the breach it is important to answer these questions.

- How did the breach occur or what was the cause of the breach?
- What programs and systems are involved?
- Is there a risk of ongoing further exposure of the information?
- How much information was collected, used or disclosed without authorization?
- How many individuals are likely to receive or have access to the information that was breached?
- What steps have been taken already to minimize the harm?
- How many people are likely to have access to the breached information and what is the likelihood of disclosure online or through the media?

- Has the information been recovered?
- Is the information encrypted or not easily accessible?
- Is there a risk for further breaches due to systemic problems or is the breach a one-time incident?
- How can the breached information be used?

Understanding how the breached information may be used is important for assessing the severity of a breach. A lost laptop with password protection and encryption that is later turned in by someone presents much less of a risk than a deliberate database intrusion. The former will likely amount to no privacy breach whereas the information in the latter is being sought after for purposeful misuse and is a breach.

2.3 Affected Individuals

Next, it is important to understand who is affected by the breach.

- Is it employees, public, contractors, clients, service providers or other organizations?
- How many individuals are, or are estimated to be, affected by the breach?

2.4 Foreseeable Harm

Identifying the risks faced by affected parties will help to inform notification and reporting decisions.

- What possible use is there for the personal information? Can the information be used for exploitation, fraud, identity theft or other harmful purposes?
- Who is in receipt of the personal information? For example, a client who accidentally receives it and voluntarily notifies the sender about the mistake is less likely to misuse the information than someone suspected of criminal activity.
- Is there a relationship between the unauthorized recipient and the individual whose personal information was breached?
- Is there a risk of significant harm to the individual such as:
    - security risks (such as physical safety)
    - identity theft or fraud
    - access to assets or financial loss
    - loss of employment or business opportunities
    - hurt, humiliation or damage to reputation/relationships
    - breach of contractual obligations
- Is there a risk of significant harm to the organization because of the breach such as:
    - loss of trust in the government
    - loss of assets (financial or otherwise)
    - financial exposure
    - loss of contracts/business/opportunity
    - legal proceedings (e.g. class action lawsuits)
- Is there a risk overall to the broader public such as:
    - risk to public health
    - risk to public safety

Step 3: Notify and Report on the Breach

3.1 Determining if Notification is Necessary

Notification to affected individual(s) may not be required for every breach. However, notification may allow affected individuals to reduce potential harm to themselves caused by the breach. To determine if notification is necessary the analysis of the nature of the breach, the amount and type of personal information involved and the potential for harm to the affected individuals are all factors to be considered.

To decide if notification is necessary the response team may consider the following:

- Contractual obligations – is there a contractual obligation to notify the affected individuals?
- Risk of identity theft – is there a possibility based on the type of information lost that this or other type of fraud could occur? Information such as name with a SIN or driver's license number could be a potential for identity theft.
- Risk of physical harm – is there a possibility that the loss could result in stalking, harassment or physical harm to the individual? Loss of child protection or criminal history information could contribute to this.
- Risk of hurt, humiliation, damage to reputation – loss of employment disciplinary records or medical information could contribute to this.
- Risk of loss of business or employment opportunities – job performance information or other types of personal evaluation documents would contribute to this.
- Legislation requires notification – the FOIPOP Act does not have provisions for notification, however, there may be other legislation that requires notification.
- Effect on the organization – is there is a possibility of loss of confidence in the organization or an impact on client relations? If so, then notification is most likely appropriate.

The **Risk Rating** chart can be used as a guide to determine where the level of risk may be. Generally, if a breach falls into the medium or high category, then most likely it will be necessary to notify the affected individuals. Use the information documented in step 2 to complete the analysis. Use the **Risk Analysis** chart in Appendix B to record the results and determine if notification to the affected individuals should occur. The final decision on notification should be done in consultation with IAP Services and the Chief Information Access and Privacy Officer.

Risk Rating Chart

Factor	**Risk Rating**		
	Low	Medium	High
Nature of personal information	- Publicly available personal information not associated with any other information	- Personal information unique to the organization that is not medical or financial information	- Medical, psychological, counselling, or financial information or unique government identification number
Relationship	- Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information	- Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information	- Disclosure to an individual with some relationship to, or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers - Theft by stranger
Cause of breach	- Technical error that has been resolved	- Accidental loss or disclosure	- Intentional breach - Cause unknown - Technical error – if not resolved
Scope	- Very few affected individuals	- Identified and limited group of affected individuals	- Large group or entire scope of group not identified

Factor	**Risk Rating**		
	Low	Medium	High
Containment efforts	- Data was adequately encrypted - Mobile device or laptop was remotely wiped and there is evidence that the device was not accessed prior to wiping - Hard copy file(s) or mobile storage device was recovered almost immediately and all files appear intact and/or untouched	- Mobile device or laptop was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping - Hard copy file(s) or mobile storage device was recovered but sufficient time passed between the loss and recovery that the data could have been accessed	- Data or device was not encrypted - Data, files or device have not been recovered - Data at risk of further disclosure particularly through mass media or online
Foreseeable harm from the breach	- No foreseeable harm from the breach	- Loss of business or employment opportunities - Hurt, humiliation, damage to reputation or relationships - Social/relational harm - Loss of trust in the public body - Loss of public body assets - Loss of public body contracts or business - Financial exposure to public body including class action lawsuits	- Security risk (e.g. physical safety) - Identify theft or fraud risk - Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances - Risk to public health or safety

3.2 When and How to Notify

For most breaches, the program/business area where the breach occurred will be responsible for notifying the affected individuals.

The method of notification should be determined by the response team. This notification should be given directly either on the phone, in person, by mail or email. Indirect notification such as general website postings or press releases should be reserved for breaches where the affected individuals are not known or a direct notification could cause further harm or a high volume makes it impracticable to notify individually. In some cases, a blended approach using multiple methods may work best, depending on the context and scope of the breach.

Generally, the notification should happen as soon as possible. However, in some cases if law enforcement is involved they should be consulted to determine if a notification would interfere with an investigation. Likewise, in rare cases if a notification may cause immediate harm to an individual's mental or physical health, alternative measures should be taken to deliver the notification, such as having it delivered via another party such as a social worker or health professional.

3.3 What to Include

The notification should give the affected individual a comprehensive set of information so that they can understand the scope and severity of a breach. This notification should include:

- Date of the breach
- Description of the breach (extent)
- Description of the information breached
- Risk to the individual caused by the breach
- Steps taken to contain the breach and any harms
- Future steps planned or any long-term plans to prevent further breaches
- Steps the individual can take to further mitigate their own risk or steps the public body has taken to assist the individual in mitigating harm. For example, how to contact credit reporting agencies or how to change a driver's license
- Contact information of a government employee who can answer questions or provide further information
- Contact information for the Office of the Information and Privacy Commissioner (OIPC) and information regarding the right to file a privacy complaint with that office. Also indicate if that office was notified of the breach.

3.5 Reporting to the Office of the Information and Privacy Commissioner (OIPC)

Currently neither FOIPOP nor PIIDPA legislation require reporting that a privacy breach has occurred to the OIPC, however, in some instances it may be advisable to do so. The Chief Information Access and Privacy Officer will guide the decision making on whether it is warranted to report to the OIPC.

Reporting will occur based on:

- sensitivity of the personal information
- whether the breached information could result in identity theft or other harm including physical harm or loss of reputation

- large number of individuals are affected by the breach
- information has not been fully recovered
- breach is a result of a systemic problem or a similar breach has occurred before

Use the risk rating analysis exercise, previously completed for notification to the affected individuals, as a guide to determine if notification to the OIPC should occur. Breaches where the analysis of the risk results in a high rating may warrant reporting to the OIPC. If a decision is made to report, use the **Report to the Office of the Information and Privacy Commissioner,** in Appendix C for this purpose.

Step 4 Investigation and Mitigation to Prevent Further Breaches

4.1 Investigation

Most likely it will be apparent how the breach occurred early in the response process. However, it is important to revisit the root cause of the breach after it has been resolved to ensure the reasons for the breach are well understood and have been rectified.

Privacy breach investigations should be led by the privacy designate/IAP administrator with the support of the program/business area leadership. As required, other areas will be engaged such as security, HR, etc. The investigation will include a review of the business practices and procedures, access controls in place, security (physical and technical), and interviews with staff involved.

The goal of the investigation is to determine what occurred, identify areas of weakness and what recommendations can be made to prevent a similar situation in the future. These recommendations may take the form of changes to physical, administrative or technical controls, changes to business processes or training and education of employees.

Depending on the scope of the breach, prior to beginning the investigation, it may be warranted to document an investigation plan. The plan should identify all possible sources of information, such as policies or procedures, that will need to be reviewed, establish scripted questions to be asked of those involved and obtain access to any system or audit logs that may be relevant.

Use the **Breach Report** form in Appendix A to record the results of the investigation.

4.2 Implement Change

Based on the findings and recommendations of the investigation, the program/business area needs to evaluate the recommendations and develop a plan for implementation. This could mean changing policy or procedures, improving security safeguards, or providing training to staff on privacy practices. The privacy designate/IAP administrator should provide input to the recommendations and follow-up to ensure that the recommendations are implemented.

4.3 Logging and Reporting

As a final step, each privacy breach should be added to a breach reporting log maintained by the privacy designate/IAP administrator. The purpose of this log is to track the breaches that have occurred. The log at a minimum should contain a brief description of the event, organization name, date of occurrence, outcome and recommended mitigations. IAP Services will compile statistics based on the logs that will be used to support statistical reporting and to help identify any trends that may be occurring which should be addressed to prevent future breaches.

For more information regarding this protocol, please contact:

Information Access and Privacy (IAP) Services
Department of Internal Services
5161 George Street, 12th Floor, Suite 1201
Phone: 902-424-2985
Email: iapservices@novascotia.ca

Appendix A

Privacy Breach Protocol

Privacy Breach Report

This form is part of the Privacy Breach Protocol. Use this form to document all actions and outcomes regarding a privacy breach.

Send the completed report and any attachments to the privacy designate/IAP administrator for recording purposes.

Contact Information	
Department/Agency	Click or tap here to enter text.
Division/Program	Click or tap here to enter text.
Completed by	
Name Click or tap here to enter text.	**Title** Click or tap here to enter text.
Preliminary Report Date Click or tap to enter a date.	**Final Report Date** Click or tap to enter a date.

Breach Details	
Date Breach Occurred	Click or tap to enter a date.
Date Breach Discovered	Click or tap to enter a date.
Date Breach Reported to IAP Administrator/Privacy Designate	Click or tap to enter a date.
Description of the Breach	
Click or tap here to enter text.	
Location of the Breach	Click or tap here to enter text.
Estimated Number of Individuals Affected	Click or tap here to enter text.

Description of Actions Taken to Contain the Breach

Click or tap here to enter text.

Description of Personal Information Breached

Click or tap here to enter text.

Description of Safeguards in Place (administrative, technical, physical)

Click or tap here to enter text.

Notification

Internal Notifications (List all individuals and position titles)

Click or tap here to enter text.

Was Notification Given to Affected Individuals? □ Yes □ No

If Yes, describe what was done and why and attach all relevant documents.
If No, describe the reason why notification was not given.

Click or tap here to enter text.

Reported to Office of the Information and Privacy Commissioner? □ Yes □ No

Describe the reason for this decision and if applicable, attach a copy of the completed Report to the Office of the Information and Privacy Commissioner Form.

Click or tap here to enter text.

Other Notifications (e.g. police, professional organization)

Click or tap here to enter text.

Investigation Findings
Click or tap here to enter text.
Recommendations to Prevent Further Breaches
Click or tap here to enter text.
Department/Agency Response to Recommendations
Click or tap here to enter text.

Appendix B

Privacy Breach Protocol

Considerations Table and Risk Recorder

This document is part of the Privacy Breach Protocol and is designed to support the decision-making activities that occur in response to a privacy breach.

Use the Considerations Table to help organize and summarize relevant and important elements/factors of the privacy breach.

Use the Risk Analysis table to document the risk analysis using the Risk Rating chart. The analysis will help to determine if notification to the affected individual(s) is necessary.

The completed form should be discussed with the privacy designate/IAP administrator to work through the next steps according to the breach protocol. The completed form should be attached to the completed Privacy Breach Report form.

Brief Description of Breach	
Click or tap here to enter text.	
Department/Agency	**Division/Program Area**
Click or tap here to enter text.	Click or tap here to enter text.
Date Breach Occurred	**Date Table Completed**
Click or tap to enter a date.	Click or tap to enter a date.
Table Completed By	**Position**
Click or tap here to enter text.	Click or tap here to enter text.

Considerations Table

Use this table to document relevant and important elements/factors of the privacy breach.

Consideration	Particulars	Check all that apply
Type of Personal Information	Age, date of birth, sex, sexual orientation, marital or family status	□
	Criminal history	□
	Educational information	□
	Employment information	□
	Financial Information (banking, credit, income, debit/credit card number)	□
	Finger prints, blood type, biometric information or other inheritable characteristics	□
	Identifying number or symbol (SIN, employee number, driver master number)	□
	Medical information, including physical or mental disability	□
	Name, address, phone number, email	□
	Race, national or ethnic origin, colour	□
	Religious or political beliefs or associations	□
	Views or opinions about the individual	□
	Other (please describe)	□
Method of Breach	Electronic system access	□
	Email/Electronic transfer	□
	Fax	□
	Hacking	□
	Incorrect mailing address	□
	Lost/stolen	□
	Social media	□
	Unencrypted Laptop, tablet or mobile phone	□
	Unencrypted USB, memory card	□
	Verbal disclosure	□
	Viewed only	□
	Other (please describe)	□
Scope of breach (number of individuals affected)	One individual	□
	Very few (less than 10)	□
	Identified and limited group (between 10 to 50)	□
	Large number of individuals (more than 50)	□
	Number affected unknown	□

Consideration	Particulars	Check all that apply
Recipient(s)	Agent/employee of government	□
	Co-worker	□
	Friend or acquaintance	□
	Individual member of the public	□
	Multiple members of the public	□
	Unauthorized family member	□
	Unknown	□
Circumstances	Existing relationship between person who breached information and the breach subject	□
	For personal gain	□
	Intentional access/use without authorization (snooping)	□
	Intentional disclosure without authorization	□
	Loss	□
	Malicious intent	□
	Theft (targeted)	□
	Theft (random)	□
	Unintentional or accidental access or disclosure	□
	Other (please describe)	□
Disposition (what happened to the information after the breach)	Believe that the information was destroyed and that no copies made, but not confirmed	□
	Confirmation of proper destruction in timely manner (e.g. shredded, deleted)	□
	Re-disclosed (e.g., to media, social media, another person)	□
	Remote wipe signal has been sent to the device but no confirmation that signal was successful	□
	Returned or recovered in full, and confirmation no copies were made	□
	Unable to retrieve electronically or in paper	□
	Unsure of location of information (device not located, papers or file not found)	□
	Viewed only, with no further access or disclosure	□
Safeguards	Data encrypted/Device encrypted	□
	Information/Data requires specialized knowledge to interpret	□
	No controls	□
	Password protected	□
	Password protected but easily determined	□
Anticipated Impact(s)/ Burden(s) of Notification to the Department	Implications for (future) trust in department/government	□
	Resources – financial	□
	Resources – human	□

Consideration	Particulars	Check all that apply
Foreseeable Harm to Affected individual(s)	Breach of contractual obligations - may require notification of third parties in the case of a data loss or privacy breach	☐
	Financial loss - when the information would allow access to financial assets such as investments or bank accounts	☐
	Hurt, humiliation, damage to reputation - associated with the loss of information such as mental health records, medical records, disciplinary records	☐
	Identity theft or fraud - most likely when the breach includes the loss of SIN, credit card numbers, driver's licence number, debit card information, etc.	☐
	Loss of business or employment opportunities - usually because of damage to the reputation of an individual	☐
	Physical harm - when the loss of information places any individual at risk from stalking or harassment	☐
Other Considerations (please describe)		☐

Risk Analysis

Use this table to document your analysis against the **Risk Rating Chart** (page 12) in the Privacy Breach Protocol.

Factor	Low	Medium	High
Nature of the personal information	☐	☐	☐
Relationship	☐	☐	☐
Cause of breach	☐	☐	☐
Scope	☐	☐	☐
Containment efforts	☐	☐	☐
Foreseeable harm from the breach	☐	☐	☐
Total Number			

Appendix C

Privacy Breach Protocol

Report to the Office of the Information and Privacy Commissioner

This form is used to submit a summary of a privacy breach to the Office of the Information and Privacy Commissioner if it is determined that a report should be submitted based on the Privacy Breach Protocol.

Contact Information	
Department/Agency:	Click or tap here to enter text.
Division/Program:	Click or tap here to enter text.
Completed by:	Click or tap here to enter text.
Title:	Click or tap here to enter text.
Report date:	Click or tap to enter a date.

Breach Description	
Date breach occurred:	Click or tap to enter a date.
Date breach discovered	Click or tap to enter a date.
Date breach reported to IAP Services:	Click or tap to enter a date.
Describe the breach and its cause Click or tap here to enter text.	
Number of individuals whose personal information was breached:	Click or tap here to enter text.
Location of the breach:	Click or tap here to enter text.
Steps taken to contain the breach: Click or tap here to enter text.	

Breach Description	
Description of personal information involved: Click or tap here to enter text.	
Description of safeguards in place at time of incident: Click or tap here to enter text.	
Notification of affected individuals:	☐ Yes ☐ No
Method of notification:	Click or tap here to enter text.
Date of notification:	Click or tap to enter a date.
Other notifications:	Click or tap here to enter text.