Canada

Protected when completed

Privacy Act Material Breach Report Form

For use by Government of Canada institutions reporting material privacy breaches to the Office of the Privacy Commissioner (OPC) and the Treasury Board of Canada Secretariat (TBS)

What is a material privacy breach?

The *Policy on Privacy Protection* defines a privacy breach as the improper or unauthorized access to, creation, collection, use, disclosure, retention or disposal of personal information. A material breach is defined as a privacy breach that could reasonably be expected to create a real risk of significant harm to an individual.

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 a credit record
- damage to or loss of property

What is personal information?

Personal information is defined in the *Privacy Act* as information about an identifiable individual that is recorded in any form including, such as:

- information relating to race, national or ethnic origin, colour, religion, age or marital status
- information relating to education, medical, criminal or employment history
- financial transactions
- any identifying number
- address, fingerprints or blood type
- personal opinions or views

Should a material breach be reported to the OPC and TBS?

Yes. Material privacy breaches must be reported to the OPC and to TBS.

I am an individual who is aware of or affected by a privacy breach. Should I use this form?

No. If you are an employee of the federal government, contact your institution’s access to information and privacy (ATIP) coordinator for guidance. If you would like to make a complaint about a breach of your privacy by an institution, consult the Report a concern section of the OPC’s website.

Who should submit this form?

The institution’s ATIP coordinator and their offices are the single liaison when notifying the OPC and TBS.

Should we include personal information in this form?

No. Do not include the names or other identifying details of affected employees or individuals.

How quickly after a material privacy breach should this form be submitted?

The *Policy on Privacy Protection* requires material privacy breaches be reported to the OPC and to TBS:

- as soon as practically possible after making efforts to contain, assess and mitigate the breach; and
- no later than seven days after the institution determines that the breach is material.

However, institutions may notify the OPC and TBS of the breach informally before the seven-day requirement. Early notification is recommended if the institution needs advice on how to manage the breach.

What can happen after a breach is reported to the OPC and TBS?

After reviewing the breach report, the OPC will contact the institution if more information is needed or to offer advice or recommend remedies. TBS advises institutions on how to manage material privacy breaches that affect two or more institutions. TBS also uses information on breaches to inform policy and guidance.

How will the OPC handle information provided by institutions in a breach report?

Under the *Privacy Act*, the OPC generally has a duty to maintain the confidentiality of breach reports submitted to the Privacy Commissioner. However, there are some exceptions to this obligation:

- the OPC is subject to access to information and privacy legislation
- the OPC may use any information, or action or inaction with respect to commitments made in response to the breach, in a potential investigation or as the basis for initiating an investigation under the *Privacy Act*
- the OPC may also disclose limited information, such as acknowledging if a breach report has been submitted, in the event of public or media enquiries, while respecting security and legal considerations

Where can I get more information on responding to a privacy breach?

For more information about responding to privacy breaches, see the OPC’s Report a privacy breach at your federal institution topic page and TBS’s Privacy Breach Management Toolkit.

All fields must be completed. Please read the instructions at the end of this form to make sure that all sections are completed and accurate.

Amended or updated reports need not have all fields completed.

Is this the first report related to this incident? (select one)

○ Original report
○ Amended or updated report

Institution's Reference Number:

For an amended or updated report, provide the existing OPC file number:

A. Information about the institution

A.1. Name of the institution

Select institution name in the drop-down list:

Institution name (if unavailable in the drop-down list):

A.2 Contact information of the institution's ATIP coordinator:

Name:

Telephone:

Telephone extension:

Email:

A.3 Contact information of a person who can answer questions about the breach on behalf of the institution:

Choose one

○ Internal representative ○ External representative (for example, a legal representative)

Name:

Title/position:

Telephone:

Telephone extension:

Email:

B. Information about the breach

B.1. Affected individuals

Number of individuals affected by the breach, if known, or the approximate number:

Additional comments (do not include any personal information)

B.2. Breach timeline

Start date (yyyy-mm-dd), or approximate start date, of breach occurrence:

Date (yyyy-mm-dd), or approximate date, on which the institution discovered the breach:

Date (yyyy-mm-dd) on which the breach was contained, if applicable:

Additional comments (do not include any personal information)

B.3. Type and cause of breach

Type of breach (select **one** option that best fits from the list below):

○ Improper and unauthorized disclosure
○ Loss
○ Theft
○ Improper and unauthorized access
○ Other (for example, overcollection or accidental deletion of personal information) (explain below)

Cause of the breach (select **one** option that best fits from the list below. Identifying the cause of the breach may require consultation with the institution’s security unit or other internal groups.)

External cause - Cyber Incident

○ Compromised credentials attack: Brute force attack
○ Compromised credentials attack: Password spray or rainbow table attack
○ Compromised credentials attack: Credential stuffing
○ Other compromised credentials attack
○ Hacking
○ Malware: Ransomware
○ Malware: Formjacking
○ Malware: Injection
○ Malware: Trojan
○ Malware: Worm
○ Other malware attack

○ Phishing
○ Other cyber incident

External cause – General

○ Misdirected correspondence: regular mail
○ Social engineering
○ Theft
○ Other external cause

Internal cause

○ Accessing information without access privileges
○ Application security vulnerability
○ Bcc field was not used
○ Classification or labelling error
○ Data entry error
○ Handling of records in an unapproved manner
○ Improper or unauthorized disposal or destruction
○ Inappropriate access rights provided
○ Loss or misplacement
○ Misdirected correspondence: regular mail
○ Misdirected correspondence: email
○ Misuse of access privileges
○ Misuse of private or entrusted knowledge
○ Theft
○ Use of workaround or shortcut
○ Use of unapproved or inappropriate hardware or device
○ Use of unapproved or inappropriate software
○ Other internal cause

Additional comments (do not include any personal information)

B.4. Description

Respond to the following questions. Do not include any personal information or information that may compromise the security of government systems. If additional information is required, the OPC or TBS will reach out to the institution.

1. Describe how and why the breach occurred (include some technical detail regarding the breach, including an explanation of the methodology if a cyber incident took place).

2. Identify all organizations and third parties, if any, involved in the breach, including their role(s) with respect to the personal information in question. Do not include the individuals affected by the breach, parties who obtained unauthorized access or unauthorized recipients or personal information.

3. Identify the physical and/or geographic location where the breach occurred, if known.

4. Describe how the breach was discovered.

5. Identify any relevant IT application(s) or system(s), if applicable

6. Identify the relevant program(s) or service(s).

7. Describe who may have had unauthorized access to the personal information (to the extent known). Include an estimate of the number of unauthorized recipients.

8. What is the relationship between the parties who had unauthorized access to the personal information, the probable recipients of the personal information and one or more of the affected individuals?

B.5. Security safeguards

Note: Completion of this section may require consultation with the institution's security unit or other internal groups. Do not include any information that may compromise the security of government systems. If additional information is required, the OPC or TBS will reach out to the institution.

Were security safeguards in place at the time of the breach to prevent it from occurring? (select one)

○ Yes ○ No ○ Unknown

If yes, specify the nature of those safeguards (select all that apply):

- □ Administrative safeguards
- □ Physical safeguards
- □ Technical safeguards

If applicable, which method(s) of physical or technical safeguards were in place? (select all that apply)

- □ Encryption
- □ IT/IM access control (for example, password, user identification, permissions, biometric identification protocol)
- □ Secure container or case
- □ Multi-factor authentication
- □ Other (specify)

Additional comments (do not include any personal information)

B.6. Personal information

Who was the personal information about? (select all that apply):

- □ Client or service recipient
- □ Federal employee
- □ Other (specify)

- □ Unknown (explain below)

To the extent known, what categories of personal information did the breach compromise? (select all categories that apply and provide elements)

Categories	**Elements of personal information** (do not include any personal information or actual numbers)
□ Account information	
□ Assigned identifying number or symbol	
□ Biometric information	
□ Contact information	
□ Credential information	
□ Demographic information	
□ Education information	
□ Employment information	
□ Financial and credit information	
□ Genetic information	
□ Government-issued information	

Categories	**Elements of personal information** (do not include any personal information or actual numbers)
□ Health information	
□ Law enforcement and administration information	
□ Location information	
□ Other information indicative of preferences, opinions or behaviour	
□ Security or surveillance information	
□ Other (specify)	

Additional comments (do not include any personal information)

Is the information subject to the breach included in a Personal Information Bank (PIB) that is registered with TBS? (select one)

- ○ Yes
- ○ No: A PIB is not required
- ○ No: PIB does not exist (for example, no legislative authority)
- ○ No: PIB is awaiting registration (PIA/PIB sent to TBS for approval)
- ○ Unknown

If applicable, identify the PIBs for the information subject to the breach. Where known, also include the TBS registration number.

Institution PIB Title and PIB Number:

TBS Registration Number:

B.7. Anticipated real risks of significant harm to an individual

What are the anticipated real risks of significant harm from the breach to any one affected individuals? (select all that apply)

- □ Bodily harm
- □ Humiliation
- □ Damage to reputation or relationships
- □ Loss of employment, business or professional opportunities
- □ Financial loss
- □ Identity theft
- □ Negative effects on the credit record
- □ Damage to or loss of property

Explain why the institution anticipates the real risk of significant harm (do not include personal information unless it is essential to explain the potential risk)

Additional comments (do not include any personal information)

C. Notification

C.1. Notification to affected individuals

Has the institution notified all affected individuals? (Answer “yes” if the notification is completed or planned). (Select one)

○ Yes ○ No

Date (yyyy-mm-dd) notification began (or is planned), if applicable:

Select one

○ Actual notification
○ Planned notification

Date (yyyy-mm-dd) notification completed, if applicable:

Method of notification used or planned for affected individuals (select one):

○ All affected individuals notified directly
○ All affected individuals notified indirectly
○ Some individuals notified directly and some individuals notified only indirectly
○ Some or all affected individuals not notified

If the institution decided against notifying some or all affected individuals, explain why.

C.2. Notification to other organizations

If applicable, which law enforcement organizations were notified about the breach (municipal, provincial, territorial, federal, international policing services)?

Name of organization(s):

Date(s) (yyyy-mm-dd) notified:

If applicable, list any other organizations or government institutions that were notified about the breach. For example, PSPC for breaches involving third-party contractors or RCMP for fraud. (Do not include institutions previously identified in this form, such as TBS.)

Name of organization(s):

Date(s) (yyyy-mm-dd) notified:

Additional comments (do not include any personal information)

D. Breach containment and mitigation

Has the institution identified the unauthorized recipients of the information? (Answer “yes” if there are no unauthorized recipients) (select one)

○ Yes ○ No ○ Unknown

If yes, has the institution contacted the recipients? (Answer “yes” if there are no unauthorized recipients) (select one)

○ Yes ○ No ○ Unknown

Does the institution or the affected individual still have access to the information that the breach compromised? (for example, a copy or backup) (select one)

○ Yes ○ No ○ Unknown

Describe any other steps taken or planned by the institution to mitigate the real risk of significant harm to individuals.

E. Breach prevention

Describe any steps taken or to be taken by the institution to reduce the risk of a similar breach from occurring in the future.

Submission of the completed form

Submit this form to the OPC and TBS through **one** of the following means:

○ By email:

Office of the Privacy Commissioner of Canada
notification@priv.gc.ca

Treasury Board of Canada Secretariat
sec@tbs-sct.gc.ca **and** ippd-dpiprp@tbs-sct.gc.ca

○ By postal mail for by hand:

Office of the Privacy Commissioner of Canada
Breach Response Unit
Compliance, Intake and Resolution Directorate
Office of the Privacy Commissioner of Canada
30 Victoria St, 1st Floor
Gatineau QC K1A 1H3

Treasury Board of Canada Secretariat
Privacy Policy Unit
Privacy and Responsible Data Division
Office of the Chief Information Officer
Treasury Board of Canada Secretariat
90 Elgin St, 4th Floor
Ottawa ON K1A 0R5

Security Policy Division
Office of the Chief Information Officer
Treasury Board of Canada Secretariat
90 Elgin St, 4th Floor
Ottawa ON K1A 0R5

If you require additional information about breach reporting requirements under the *Directive on Privacy Practices*, contact the TBS Privacy and Responsible Data Division by sending an email to ippd-dpiprp@tbs-sct.gc.ca.

Instructions for completing the *Privacy Act* Material Breach Report Form

All fields must be completed, and the form must be submitted to the OPC and TBS no later than seven days after the institution determines that the breach is material.

Once completed, this form should be marked and safeguarded using the appropriate classification level. The form should be labelled “Protected B” if personal information is included.

A.1 Name of the institution: Consult the Federal Identity Program registry of applied titles.

A.3 Coordinates of a contact other than the ATIP coordinator: Enter the information of any contact other than the institution’s ATIP coordinator who can answer questions about the breach on behalf of the organization.

B.1. Number of individuals affected by the breach, if known, or the approximate number: Indicate the number of individuals whose personal information has been or may have been compromised through the breach. If the exact number is not known, enter the approximate number and add a note in the comments section. Update this information in an amended report if the exact number becomes known.

Tip: For more information about what constitutes personal information, see the OPC’s The *Privacy Act* in brief web page.

B.2. Breach timeline: Enter the date when the breach started. If uncertain, enter the earliest date when the breach could possibly have started. For example, if misdirected mail caused the breach, enter the date on which the mail was sent.

“When the institution discovered the breach” refers to when the breach was first discovered, for example, by any employee of the OPI. This date of discovery may be before the date the departmental ATIP coordinator or chief security officer learned about the breach.

If the breach is contained, which means that the institution deems that the information is not vulnerable to further improper or unauthorized access, disclosure or use, add the date the breach was contained. The date the breach was contained is indicated as “if applicable” because it may not be possible to contain the breach. As appropriate, institutions may submit an updated report with additional details about containment measures following their completion.

Tip: For more information about breach containment, see TBS’s Privacy Breach Management Toolkit.

B.3. Type and cause of breach: This information is important for determining the real risk of significant harm to an individual and how to mitigate that harm. Institutions should identify only one cause of the breach, even if other related events aggravate the harm associated with the breach. Any secondary or aggravating events related to the breach should be identified in the “additional comments” box so that the full context of the breach can be understood.

Below are explanations of the types of breaches used in this form. These types generally correspond to related terminology commonly used in the information technology (IT) and security communities. Other types of breaches are captured in the fifth row and require separate consideration on how they relate to IT/security terminology.

Type of breach	Related terminology commonly used in IT and Security communities
Improper and unauthorized disclosure occurs when personal information is disclosed by the institution (including third parties acting under arrangement, agreement or contract with the institution), whether intentionally or unintentionally, to a recipient without a “need to know”. This disclosure can occur externally or internally within an institution. Examples could include: • accidental display of personal information to employees (e.g. on a PowerPoint presentation or access permissions being set too broadly) • incomplete de-identification prior to sharing personal information • improper or incomplete application of severances or redactions before disclosing personal information • misdirected unencrypted emails	This generally corresponds to the IT/security term - **confidentiality breach** - that includes the inappropriate or unauthorized disclosure of information.
Loss occurs when the institution (including third parties acting under arrangement, agreement or contract with the institution) loses control over personal information through the actions of its employees or partners, such that the institution no longer has continued access to the personal information. A loss may result in an unauthorized party gaining access or control over the information. This is unintentional on the part of the institution and the recipient. Examples could include: • mail delivery to the wrong address • disposal or sale of equipment or devices without first purging them of personal information loss of equipment or files during a move or as a result of being misplaced	This generally corresponds to the IT/security term – **availability breach.** It could also correspond to the IT/security term **confidentiality breach** if there is inappropriate or unauthorized access to the lost information.
Theft occurs when an unauthorized party intentionally takes control of personal information such that the institution no longer has access to it. Examples could include: • theft of equipment or device that is insufficiently encrypted • removal of paper files from the institution	This generally corresponds to **confidentiality breach**. It could also correspond to – **integrity breach** – where the information is unusable or **availability breach –** where the information is inaccessible.

Improper and unauthorized access occurs when an unauthorized party (without a “need to know”), through their own actions, accesses personal information. Their actions may be intentional or unintentional.

Examples could include:

- employee “snooping” or other abuse of access privileges
- cyber attacks, for example ransomware, malware

This generally corresponds to the IT/security term - **confidentiality breach** - that includes the unauthorized or inappropriate access to information. It could also correspond to – **integrity breach** – where the information is modified.

Other breaches of sections 4-8 of the *Privacy Act*, including improper or unauthorized collection, use, creation, retention of personal information.

Examples could include:

- collecting or creating personal information that is not directly related to a program or activity
- using personal information for an unauthorized purpose
- accidental or premature deletion or disposal of personal information
- Not disposing personal information according to established disposal schedules

Other breaches should be considered individually regarding how they relate to IT and security terminology.

Cause of the breach: This information is important for deciding on steps to prevent a reoccurrence of the breach. This form groups the causes of breaches into three categories:

External cause – Cyber incident: any unauthorized attempt to gain access to, modify, destroy, delete or render unavailable any computer network or system resource.

> **Tip:** For more information about cyber incidents, consult appropriate groups in your institution and see the Canadian Centre for Cyber Security’s Glossary and TBS’s Privacy Implementation Notice 2022-01: Cyber security incidents involving personal information.

- **External cause– General:** includes social engineering and theft.
  Tip: For more information about social engineering, see the OPC’s Deceptive and manipulative: social engineering techniques page.

- **Internal cause:** refers to actions by employees of the institution, as well as third parties acting under arrangement, agreement or contract with the institution. The list of causes covers both intentional and unintentional actions.
  Tip: For more information about causes in this category, see the following resources on the OPC’s website:
  - Key privacy protection tips for federal human resources professionals
  - Ten tips for addressing employee snooping
  - Tips for federal institutions using portable storage devices

B.4. Description: Provide as much detail as possible under each question, without including personal information. If additional information is required, the OPC or TBS will reach out to the institution. For questions that are not applicable to the breach, indicate “not applicable” on the form.

Notes regarding questions 2, 3, 6 and 8:

2. This question is to identify any third parties involved in the breach, such as contractors or other federal institutions, and to establish their role in the breach. This question is not intended to identify the individuals affected by the breach, parties who obtained unauthorized access or unauthorized recipients or personal information.
3. Provide detailed information on the geographic location of the breach (region within Canada, abroad and so on) and on the physical location where the breach occurred (for example, mailroom, stolen from a vehicle). For example, if the breach was caused by lost mail, indicate the origin, the intended destination, and any known information about where the mail was lost.

6. This question is to establish the institutional initiative under which the breach occurred (for example, a benefits program). This question is not intended to identify IT applications or systems.

8. This question is to identify any relationships between the parties who had unauthorized access to the personal information, the probable recipients of the personal information and one or more of the affected individuals. The relationship may be professional or personal. This information may be important for determining the real risk of significant harm to an individual and how to mitigate that harm.

B.5. Security safeguards: This question is to establish the security safeguards that were in place when the breach occurred. This information is important for deciding on steps to prevent a reoccurrence of the breach. For ease of use, this form refers to the types of security safeguards mentioned in the *Directive on Privacy Practices* and the *Policy on Government Security*.

Type of security safeguard	Examples
Administrative safeguards	Institutional security policy; security provisions in a service contract for the destruction of records
Physical safeguards	Locked storage rooms, locked filing cabinets
Technical safeguards	Encryption; electronic access control devices, audit controls

Tip: For more information about the types of safeguards, see:

- Appendix A in the *Directive on Privacy Practices*
- The *Directive on Security Management*, including:
  - Appendix B: Mandatory Procedures for Information Technology Security Control
  - Appendix C: Mandatory Procedures for Physical Security Control
  - Appendix E: Mandatory Procedures for Information Management Security Control

B.6. Who was the personal information about? In addition to specifying whether the breach affected clients, service recipients or federal employees, you are encouraged to use the “other” option to report additional relevant information about the affected individual(s), to the extent known. For example, is the affected individual(s) part of a group that may be particularly susceptible to injury or harm from the breach, such as a minor, a victim of crime or a person in a vulnerable economic situation? This information is important because it informs the assessment of the real risk of harm to an individual.

The “other” category could also include survey respondents, working group participants or social media commentators.

What categories and types of personal information did the breach compromise, to the extent known? Review the categories to determine the scope of the information that the breach compromised. Next, enter all the types of information that the breach compromised. For example, types of health information could include a medical history or a medical record (for example, a prescription or a test result). “Contact information” could include name, phone number, mobile number, email address, civic address, postal code, city of residence and previous addresses. “Demographic information” could include ancestry data, date of birth, educational history, marital status, gender, ethnic origin or nationality.

Including this information will help ensure that the form is complete.

Personal information banks (PIBs) and TBS registration number: If the personal information subject to the breach was collected for an administrative purpose, identify the relevant PIB(s) by providing the PIB title, PIB number, and the TBS registration number. If the relevant PIB(s) is not known at the time of the initial report, provide an update as soon as possible. Occasionally, the personal information subject to the breach may not have been intended to be used for an administrative purpose, for example, information that was collected incidentally from unsolicited correspondence is not part of a decision-making process. In these cases, the information would not be captured in a PIB, so no PIB number can be quoted. If there is no applicable PIB or the relevant PIB is unknown at the time of the initial report, indicate “not applicable” or “unknown” where the PIB title and number are requested.

B.7. Anticipated real risks of significant harm to an individual: A material privacy breach could reasonably be expected to create a real risk of significant harm to an individual. For ease of use, this form lists the types of significant harm set out in the *Policy on Privacy Protection* and offers examples of means that could enable the harms. The types of harm and examples of means provided below are illustrative, not exhaustive.

Types of significant harm	Examples of means that could enable harms
Bodily harm	Blackmail; identity fraud; physically locating and/or communicating with an individual such that it enables a criminal offence (e.g., involving threats or physical harm)
Humiliation / Damage to reputation or relationships	Public shaming
Financial loss / negative effects on the credit record / loss of employment, business or professional opportunities	Blackmail; bank account fraud; financial exploitation; identity fraud; payment card fraud; public shaming
Identity theft	Phishing
Damage to or loss of property	Loss of records; phishing; physically locating and/or communicating with an individual such that it enables a criminal offence (e.g., involving threats or physical harm)

Tips

- For more information about assessing the risk of harm to an individual, see the TBS Privacy Breach Management Toolkit

C.1. Notification to affected individuals: The *Directive on Privacy Practices* requires institutions to include the notification of individuals affected by a privacy breach in the mitigation measures they must enact in response to a material privacy breach, unless notification would be inappropriate for security, confidentiality, legal or other reasons.

- **Direct notifications** can occur by telephone, email, letter or in person

- **Indirect notifications** refer to notifications made via information posted on the institutional website or social media accounts, posted notices, or the media

The method chosen will depend on the circumstances and should be determined by the institution on a case-by-case basis. Indirect notification should generally be used only when the individuals cannot be located or when there are so many individuals that direct notification would be untimely or too costly.

C.2. Notification to other organizations: If a breach affects personal information that is held by the institution but is not under its control, the *Directive on Privacy Practices* requires the institution to promptly notify the organization that controls the personal information. If more than one organization is listed, number them and use that reference number when listing the date they were notified in the field below. For more information about notifying other organizations, see Appendix I: Standard on Security Event Reporting of the *Directive on Security Management*.

D. Breach containment and mitigation: Question B.2 concerns immediate breach containment (that is, stopping the breach). Section D concerns the institution's subsequent and ongoing breach containment and mitigation action, including contacting unauthorized recipients, where appropriate and safe to do so, to try to retrieve any documents or copies of documents that the breach compromised.

In addition to listing containment measures, include any actions taken or planned to mitigate the real risk of significant harm to an individual. Examples include:

- resetting passwords
- offering credit monitoring services where appropriate
- recovering misdirected information
- seeking confirmation from unintended recipients that they have destroyed and not circulated the information
- notifying third parties that can reduce the risk of harm, such as payment processors, institutions that issued documents that were compromised, and institutions that may use the compromised information for administrative decisions

This information is particularly important when the OPC determines where it should offer advice or recommend remedies. Update this information in an amended report if there are any changes between the planned actions and the final breach containment and mitigation actions taken by your institution.

E. Breach prevention

Tip: For more information about preventing and responding to a privacy breach, see:

- the TBS Privacy Breach Management Toolkit
- Preventing and responding to a privacy breach on the OPC's website