# OPI Preliminary Breach Report Form

Phase 1: Identify and contain the breach

This report can be completed by the office of primary interest (OPI) for the program area of the federal institution where a privacy breach has been discovered to meet their obligation to notify privacy officials of potential or confirmed privacy breaches. Often the employee who first identifies the breach will be responsible for reporting it to privacy officials. If there are security implications, the report can also be used to notify the institution’s security officials.

Do not include personal information in this report unless it is necessary to explain the nature and sensitivity of the personal information involved. If personal information is included, be sure to label the document as “Protected B”.

## A. Information about the office of primary interest (OPI)

**Date (yyyy-mm-dd) the report was completed by the employee** (required)**:**

**Report completed by** (required)**:**

Name:

Position:

Telephone:

Email:

## B. Details of the breach

1. Provide the date(s) (yyyy-mm-dd) and time of the (potential) breach (required):

[Insert text here]

2. Provide the location of the (potential) breach (required):

[Insert text here]

3. When and how was the breach or potential breach discovered?

[Insert text here]

4. Provide a brief description of the breach or potential breach, including how the breach occurred, the type of personal information affected (for example, health, financial) and the number of individuals affected or potentially affected (required):

[Insert text here]

5. Describe the format of information involved – electronic, paper records, other (describe):

[Insert text here]

6. Describe the security classification of the information (Unclassified, Protected A, Protected B, Protected C / Confidential, Secret, Top Secret):

[Insert text here]

7. To the extent known, what personal information elements were involved (for example, social insurance number, age, marital status)?

[Insert text here]

8. List the immediate containment actions and/or interventions taken, if any (required):

[Insert text here]

9. Describe any information or evidence that suggests a breach has occurred. If there is uncertainty as to whether the incident constitutes a privacy breach, describe any information that suggests a privacy breach has not occurred:

[Insert text here]

## C. Individual(s) affected

1. Provide a description of the individuals affected by the breach (for example, applicants to program A, employee of division B).

[Insert text here]

2. Are these individuals aware of the breach?

[Insert text here]

## D. Individual(s) involved

**Provide information about the individuals involved in the breach** (for example, employee who discovered the breach, their supervisor, witnesses; attach list if necessary)

### Individual 1

Name:

Title/position:

Telephone:

Email:

How was this person involved?

[Insert text here]

### Individual 2

Name:

Title/position:

Telephone:

Email:

How was this person involved?

[Insert text here]

## E. Next steps (to be completed by privacy officials on receipt)

1. Is a full assessment of the breach required? (Unless the preliminary breach report provides sufficient information to [rule out a material breach](https://056gc.sharepoint.com/:w:/r/sites/DigitalAdvisoryServices-Serviceconsultatifscontenunumrique/_layouts/15/Doc.aspx?sourcedoc=%7B9871E823-E49F-4DE5-B5F0-24143C671996%7D&file=1%20-%20Identifying%20a%20privacy%20breach%20-%20definitions%20and%20scenarios.docx&action=default&mobileredirect=true), a full assessment will likely be required. A full assessment may also be needed to determine appropriate mitigation and prevention measures.)

[Insert text here]

2. If applicable, explain why a full assessment is not required:

[Insert text here]

3. Name of the privacy official that completed the report:

4. Date (yyyy-mm-dd) the report was completed by the privacy official: