|  |
| --- |
| **For ATIP use** |
|  |

**PRIVACY BREACH REPORT AND RISK ASSESSMENT**

|  |
| --- |
| **Privacy statement:** Personal information in this report is collected under the authority of the *Financial Administration Act* and/or the *National Defence Act*.The information is required to report and investigate privacy and security breaches, and to ensure that vulnerabilities are identified and the risk of future occurrences is reduced. Personal information is protected and only used and disclosed in accordance with the *Privacy Act*, and as described in personal information bank PSU 939 [Security Incidents and Privacy Breaches](http://www.infosource.gc.ca/emp/emp03-eng.asp#psu939). Under the Act, individuals have right of access to, and correction of, their personal information, and the right to file a complaint to the Privacy Commissioner of Canada regarding the handling of their personal information. For more information consult the [*Info Source*](http://www.infosource.gc.ca/). |

**Instructions:**

1. Upon discovery of an actual or suspected privacy breach that involves personal information, the **Office of Primary Interest (OPI)** must contain the breach and immediately report it in accordance with the Canadian Forces Morale and Welfare Services (CFMWS) Privacy Breach Protocol*.*
2. The OPI must promptly send this report to the CFMWS National Manager Access to Information and Privacy Program (NM ATIP) at ATIP.AIPRP@cfmws.com.

Part I can be sent separately prior to submitting the other parts.

Part II is to be sent as soon as possible following discovery.

NM ATIP can assist you in completing the report.

1. The NM ATIP will liaise with the OPI contact or other designated individual and with Security, as appropriate, and will also advise the CFMWS Vice-President Corporate Services (VP CorpSvcs).

**PART I: PRIVACY BREACH REPORT**

**Contact information:**

|  |  |
| --- | --- |
| **Date reported to ATIP** | YYYY-MM-DD |
| **ATIP contact** | Rachelle DelageCFMWS NM ATIP4210, Labelle St, Ottawa, ON K1A 0K2ATIP.AIPRP@cfmws.com, 613-943-0018 |
| **OPI contact** | NameTitleAddressEmail, telephone |
| **Other contacts, if applicable** (i.e. Security, internal investigation, other) | NameTitleAddressEmail, telephone |

**Details of the incident:**

|  |  |
| --- | --- |
| **Date of the breach** | YYYY-MM-DD |
| **Description of the breach** (e.g. cause, technological issues involved, location, geographical area affected, and discovery) | *What happened, how it happened, when and how discovered, etc.* |
| **Number of affected individual(s)**  |  |
| **Status of individuals affected** (e.g. employees, contractors, public, clients) |  |
| **Do parties know each other?** (e.g. co-workers, ex-spouses) |  |
| **How broadly had the personal information been disclosed?** |  |
| **Has any other organization been notified of the breach? If so, when?** (e.g. law enforcement, other) |  |
| **Is there any other investigation related to the breach?** (e.g. security, criminal) |  |

**Actions anticipated or taken following the breach:**

|  |  |
| --- | --- |
| **Measures taken to stop/ contain the breach** | *Complete the* ***Privacy breach checklist*** |
| **Has the information been recovered? If not, explain what steps are being taken.** |  |
| **Have affected individuals been notified of the breach and of their right to complain to the Office of the Privacy Commissioner, or will they be notified?** (e.g. by letter, telephone) |  |
| **Measures contemplated or being taken to prevent a recurrence** (e.g. training, new policies or procedures) |  |

**Additional information:**

|  |
| --- |
| **Context** |
| **Type of personal information** |
| [ ]  Name[ ]  Biographical information [ ]  Biometric information[ ]  Citizenship status[ ]  Contact information[ ]  Credit information [ ]  Criminal checks/history[ ]  Date of birth[ ]  Date of death [ ]  Educational information[ ]  Employment equity information | [ ]  Employee identification[ ]  Employee personnel information [ ]  Financial information[ ]  Medical information[ ]  Physical attributes[ ]  Place of birth[ ]  Place of death [ ]  Signature[ ]  Social Insurance Number [ ]  Other identification numbers [ ]  Other:  |
| **Sensitivity of the information** (If unsure, consult Security) |
| [ ]  Protected A(Low sensitive – injury) | [ ]  Protected B(Particularly sensitive –serious injury) | [ ]  Protected C(Extremely sensitive – life threatening and/or extremely grave injury) |
| **Format of the information**[ ]  Paper (mail, sensitive waste, etc.)[ ]  Electronic (email, website, database, laptop, tablet, USB key, CD-ROM, etc.)[ ]  Other

|  |
| --- |
| Details:  |

 |
| **Security measures in place at the time of the breach**[ ]  Technical (encryption, password, etc.)[ ]  Physical (locks, alarm systems, etc.)[ ]  Organizational (security clearances, policies, training, contractual provisions, etc.)

|  |
| --- |
| Details:  |

 |
| **Expectation of the affected individual(s)**[ ]  Is there a privacy statement? Is it clear and comprehensive (e.g., does it list the statutory authority for the collection, the right to refuse, and the right of access and correction)? [ ]  Was the use and disclosure in accordance with the purpose of initial collection (e.g., statistical, program administration)? [ ]  Was consent given to preclude some or all types of disclosure? (Note that consent does not replace authority to collect.) [ ]  Are there disclosure provisions to third parties (e.g., is there a commitment not to disclose information unless authorized)? [ ]  Are disclosures accurately reflected in a Personal Information Bank published in *Info Source*? [ ]  Other

|  |
| --- |
| Details:  |

 |
| **Individual(s) affected by the breach – Attach list if necessary**(Name and coordinates, or PRI or other identifier, if applicable)*To be provided in paper copy only, if required.* |
| **Individual(s) directly involved in the breach – Attach list if necessary**(Name and coordinates of witness(es), investigator, what was their role in the breach and how they were involved.)*Do not include name of individual(s) who may have caused the breach.**To be provided in paper copy only, if required.* |
| **Additional information / comments:** |
|  |
| **Follow-up** |
| [ ]  The OPI has determined that the privacy breach has been addressed internally, with no follow-up required. | Date closed:YYYY-MM-DD |
| [ ]  NM ATIP agrees with OPI and file closed. | Date closed: YYYY-MM-DD |
| ***Parts II and III to be completed if risk assessment required*** |

**PART II: RISK ASSESSMENT**

|  |
| --- |
| **A: Risk impact to the individual(s)** |
| 1. **Financial Loss**

[ ]  Identity theft or fraud [ ]  Inconvenience due to changing financial arrangements[ ]  Loss of wages or of job or employment opportunities (loss of promotion)[ ]  Loss of business opportunities[ ]  Increased cost or loss of insurance[ ]  Pension loss[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Health**

[ ]  Physical safety (security risk) [ ]  Physiological impact (loss of sleep, stomach problems, heart attack, long-term medication regime)[ ]  Psychological impact (stress, breakdown of relationships)[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Reputation**

[ ]  Hurt, humiliation or embarrassment[ ]  Discrimination[ ]  Loss of professional standing[ ]  Loss of personal standing[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Legal**

[ ]  Civil charges[ ]  Criminal charges[ ]  Fines[ ]  Imprisonment[ ]  Possible application of foreign laws (potential for disclosure to a foreign government for unrelated use)[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
|  |
| **B: Risk impact to the institution** |
| 1. **Reputation**

[ ]  Call for the resignation of the minister and/or departmental officials [ ]  Scrutiny by parliamentary officials[ ]  Increased public scrutiny (Question Period) [ ]  Criticism by central agencies[ ]  Funding revisited[ ]  Internal investigation[ ]  Loss of public trust [ ]  National embarrassment[ ]  Public inquiry[ ]  Investigation and/or audit by OPC[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Financial**

[ ]  Loss of funding for program(s) or activity[ ]  Reallocation of resources and assets[ ]  Changes to Program Activity Architecture[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Legal**

[ ]  Lawsuit or fines[ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability of occurrence** |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **National Interest**

[ ]  Threat to public health [ ]  Threat to public safety[ ]  Threat to national security[ ]  Negative impact on federal-provincial-territorial relations[ ]  Negative impact on international relations [ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |
| 1. **Operations**

Will the breach result in:[ ]  Decrease in uptake of services[ ]  Decrease in staff morale resulting in decreased productivity and increased turnover[ ]  Calls for replacing the minister or head[ ]  Sanction or firing of employees[ ]  Program redesign or cancellation[ ]  Relocation of employees[ ]  Increased administration and overhead[ ]  Interruption of service delivery[ ]  Increased public scrutiny negatively affecting business operations [ ]  Other:  |
| **Impact rating** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
| **Probability**  |
| [ ]  N/A | [ ]  Unlikely | [ ]  Rare | [ ]  Likely | [ ]  Very likely | [ ]  Almost certain |
| **Comments:**  |

**PART III: RISK ASSESSMENT SUMMARY AND RECOMMENDATIONS**

The determination of an overall risk level is based on the highest of the impact ratings identified in part II A and B. ***Part III to be completed by ATIP.***

|  |
| --- |
| **A: Risk impact to the individual(s)—Summary** |
| **Category** |
| [ ]  Financial | [ ]  Health | [ ]  Reputation | [ ]  Legal |
| **Overall risk level** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
|  |
| **B: Risk impact to the institution—Summary** |
| **Category** |
| [ ]  Reputation | [ ]  Financial | [ ]  Legal | [ ]  Nat’l interest | [ ]  Operational |
| **Overall risk level** |
| [ ]  N/A | [ ]  Negligible | [ ]  Low | [ ]  Moderate | [ ]  High | [ ]  Severe |
|  |
| **C: ATIP recommendations** |
| **Notification – External** |
| [ ]  Affected individual(s) | [ ]  OPC and TBS | [ ]  Other(s): |
| [ ]  No external notification (explain why):  |
| **Notification – Internal** |
| [x]  Security (always) | [ ]  DGMWS | [ ]  CDS and/or CMP |
| [ ]  IM/IT | [ ]  Division Head | [ ]  Minister’s office |
| [ ]  Legal Advisor | [ ]  Public Affairs | [ ]  Other(s): |
| **Additional recommendations / comments** [ ]  Training, education and awareness sessions[ ]  Review of internal policies or procedures[ ]  Improvements to infrastructure and systems[ ]  Privacy impact assessment (PIA)[ ]  New or revised Personal Information Bank (PIB)[ ]  Review of privacy notice and consent statement[ ]  Follow-up audit[ ]  Other:  |

**RISK MATRIX**

|  |  |  |
| --- | --- | --- |
|  |  | **Probability of occurrence** |
|  |  | **Rare****(Very infrequent)** | **Unlikely****(Infrequent)** | **Likely****(Occasional)** | **Very Likely****(Frequent)** | **Almost certain (Continuous)** |
| **Impact rating** | **Severe** | **Significant** | **Major** | **High** | **Severe** | **Severe** |
| **High** | **Moderate** | **Significant** | **Major** | **High** | **Severe** |
| **Moderate** | **Low** | **Moderate** | **Significant** | **Major** | **High** |
| **Low** | **Negligible** | **Low** | **Moderate** | **Significant** | **Major** |
| **Negligible** | **Negligible** | **Negligible** | **Low** | **Moderate** | **Significant** |

|  |  |  |  |
| --- | --- | --- | --- |
|  | **Low Risk Zone** | **Medium-Risk Zone** | **High-Risk Zone** |

| **POTENTIAL IMPACTS TO THE INSTITUTION** |
| --- |
| **Impact rating** | **Reputation and relationships with clients and the public** | **Legal and policy compliance** | **National interest, public safety and security** | **Operations and capacity to deliver programs** | **Financial resources and assets** |
| **Severe**Event consequences require the organization to make a large-scale, long-term realignment of operations, objectives or finances | Complete loss of public trust Embarrassment for the minister or the government  | Non-compliance with various Government of Canada laws or policies may result in substantial legal liabilities or penalties (civil or criminal) and/or imprisonment | Extensive impacts on federal-provincial-territorial and/or international relationships, resulting in threats to public safety and securityNational security put in jeopardy | Consequences threaten survival of program and organizationService interruption of more than six months | Loss, error or omission of greater than $25 million, or greater than 25 per cent of total managed funds |
| **High**Event consequences can be endured by the organization but could result in significant impact | Significant loss of client group trustPublic outcry for removal of the minister and/or departmental officialsSubject to an audit and/or investigation by the Office of the Privacy Commission (OPC)Strong criticism by central agenciesScrutiny by a parliamentary committee | Non-compliance with Government of Canada laws or policies may result in significant legal liabilities or penalties (civil or criminal), such as a lawsuit | Substantial impact to federal-provincial-territorial and/or international relationshipsSubstantial impact on public safety and security | Consequences threaten survival and continued effective functioning of the program, or require intervention by senior management or by elected representativesService interruption of one to six months | Loss, error or omission of between $15 million to $25 million, or between 25 per cent and 15 per cent of total managed funds |
| **Moderate**Event consequences can be absorbed with proper management to minimize the impact | Some loss of client group trustMedia outcry for replacement of the minister and/or departmental officialsModerate criticism by central agencies | Non-compliance with Government of Canada laws or policies, which may result in limited legal liabilities or penalties (civil or criminal), such as a lawsuit | Disruption to federal-provincial-territorial and/or international relationshipsModerate impact on public safety and security | Consequences do not threaten the program, but administering the program could be subject to significant review or change in operationService interruption of up to a month  | Loss, error or omission of between $5 million to $15 million, or between 15 per cent and 5 per cent of total managed funds |
| **Low**Event consequences can be absorbed with managed effort  | Setback in building of client group trustNegative media attentionMay be subject to an investigation by OPC Minor criticism by central agencies and/or OPC | Non-compliance with Government of Canada policies without legal liabilities or penalties (civil or criminal) | Minor disruptions to federal-provincial-territorial relationshipsMinimal impact on public health and security  | Consequences threaten efficiency or effectiveness of some aspects of the program but can be dealt with internallyService interruption of one day to one week  | Loss, error or omission of between $1 million to $5 million, or between 1 per cent and 5 per cent of total managed funds |
| **Negligible**Event consequences can be absorbed through normal activity | No relationship damageSome unfavourable media attentionSome unfavourable observation by central agencies and/or OPC | Non-compliance with Government of Canada policies without legal liabilities or penalties (civil or criminal) | Negligible impact on federal-provincial-territorial relationshipsNegligible impact on public safety and security | Consequences are dealt with through routine operationsService interruption of less than a single day  | Loss, error or omission of less than $1 million, or less than 1 per cent of total managed funds |

**NOTIFICATIONS REQUIREMENTS**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Breach impact**  | **Division Head** | **VP****CorpServ** | **DGMWS** | **CDS and/or CMP** | **Minister’s office** | **OPC and TBS** | **Affected individuals** |
| **Low**  | May be informed  | May be informed | May be informed  | May be informed  | May be informed  | May be informed  | **Must** be informed(within 5 working days) |
| **Moderate** | **Must** be informed  | **Must** be informed  |
| **High**  | **Must** be informed  | **Must** be informed  | **Must** be informed  | **Must** be informed | **Must** be informed(NM ATIP to determine timing) |
| **Severe**  |
|  |  |  |  |  |  |  |  |
| **Responsibility** | OPI | NM ATIP | VP CS | DGMWS | DGMWS via CDS and/or CMP | NM ATIP | OPI |
| **Form of notification** | Verbal | Verbal | Verbal | Verbal and/or Briefing Note  | Briefing Note | *Privacy Act* Breach Report by email | Letter |