Privacy Breach Protocol

DATE OF ISSUE: September 2017
REVISION DATE: N/A

APPLICATION

1. This is an order that applies to members of the Canadian Armed Forces and a directive that applies to employees of the Department of National Defence (DND) and to the Staff of the Non-Public Funds (NPF), Canadian Forces (CF) involved in the administration and delivery of Non-Public Property (NPP) activities, services and programs.
2. For greater certainty, this includes all non-public property vested in the commanders of units and other elements, and in the Chief of the Defence Staff (CDS) established under sections 38 to 41 of the *National Defence Act*; all activities of the Staff of the NPF, CF; and all non-public property services, programs and operations including those public Alternative Service Delivery functions assigned to be executed under the NPP accountability framework.

APPROVAL AUTHORITY

3. This protocol is issued under the authority of the Director General Morale Welfare Services (DGMWS), in his capacity as the Managing Director NPP and Chief Executive Officer (CEO), Staff of the NPF, CF.

ENQUIRIES

4. Enquiries should be directed to the Canadian Forces Morale and Welfare Services (CFMWS) National Manager Access to Information and Privacy Program (NM ATIP).

DEFINITIONS

5. Consult Annex A: Definitions.

POLICY OBJECTIVE

6. CFMWS management and staff at all levels must take all necessary steps to ensure privacy is a high priority and where possible mitigate the risk of a privacy breach. Without a timely and proper response to any suspected or actual privacy breach, there is a risk that there will be significant damage to the CFMWS organizational reputation and compromise of personal information.

PROCEDURES

7. Consult Annex B: Procedures for responding to a privacy breach.

MONITORING AND CONSEQUENCES

8. The monitoring and consequences outlined in the CFMWS Policy on privacy practices apply to this protocol.

REFERENCES

Acts and regulations:

a. *Privacy Act*
b. *Privacy Regulations*

Treasury Board publications:

a. Policy on Government Security
b. Policy on Privacy Protection
c. Directive on Privacy Practices
d. Guidelines for Privacy Breaches

CFMWS policies:

a. Policy on the Access to Information and Privacy (ATIP) Program
b. Policy on Privacy Practices
c. Security Orders

ANNEXES

Annex A: Definitions

Annex B: Procedures for responding to a privacy breach

ANNEX A: DEFINITIONS

Compromise: The unauthorized access to or disclosure, destruction, removal, modification, use or interruption of information.

Disclosure: Release of personal information by any method (e.g., transmission, provision of a copy, examination of a record) to any body or person.

Need-to-know: The restriction of access to protected or classified information to individuals who need to access and know the information in order to perform their duties.

Non-Public Property: NPP is defined in section 2 of the *National Defence Act* (NDA) and includes all money and property received for or administered by or through NPP organizations, and all money and property contributed to or by CAF members for their collective benefit and welfare.

Personal information: Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the *Privacy Act*. Examples include information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual.

Privacy: The right of an individual to be left alone, to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information.

Privacy breach: The improper or unauthorized creation, collection, access, use, disclosure, retention and/or disposal of personal information. A privacy breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Protected information: Information that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act* because its disclosure would reasonably be expected to compromise the non-national interest.

Material privacy breach: A privacy breach that involves sensitive personal information and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals.

Risk: The uncertainty that can create exposure to undesired future events and outcomes. It is the expression of the likelihood and impact of an event with the potential to impede the achievement of an organization's objectives. The classic formula for quantifying risk combines magnitude of damage and probability is as follows: risk = probability × impact.

Unauthorized access: Access to information by an individual who is not properly security screened and/or does not have a need-to-know.

Unauthorized disclosure: A disclosure that is forbidden by law or by governmental or departmental regulations, directives or policies.

Uncertainty: The state of full or partial deficiency of information necessary to understanding or knowing of an event, or its likelihood or consequences.

ANNEX B: PROCEDURES FOR RESPONDING TO A PRIVACY BREACH

STEP 1: DISCOVERY AND REPORTING

Notice: *Upon learning of an actual or suspected privacy breach, immediate action must be taken to stop and report the breach. Reporting may occur through different means; initially, this may be done through verbal communication. Suspend the process or activity that caused the actual or suspected privacy breach. Stopping the breach and reporting should occur simultaneously wherever possible.*

Office of primary interest (OPI)

1.1. Immediately stop/contain the breach and secure the compromised records, systems or websites, in order to prevent further theft, loss or unauthorized access, use, disclosure, copying, modification or disposal of personal information. Suggested containment strategies are found in the **Privacy breach checklist** (see Appendix 1 of Annex B).

1.2. Promptly report the breach to the Canadian Forces Morale and Welfare Services (CFMWS) National Manager Access to Information and Privacy Program (NM ATIP), i.e. within 24 hours (1 working day) of becoming aware of any actual or suspected privacy breach.

This can be done verbally followed by an email to **ATIP.AIPRP@cfmws.com** along with **Part 1 of the Privacy breach report and risk assessment (PBRRA)** (see Appendix 2 of Annex B). Include the following elements in the report to the extent possible:

- when (date) and how was the breach discovered;
- a description of the incident, including date and location;
- the cause (if known);
- individuals/parties who it is believed committed the breach or may be involved in the breach (internal and/or external);
- a description of the compromised data;
- the number of individuals affected by the breach;
- measures taken to stop/contain the breach
- whether the information was recovered;
- the vulnerability of CFMWS and affected individuals;
- who was notified;
- measures taken or contemplated to prevent a recurrence;
- security issues considered; and,
- any other relevant information.

The **Privacy breach checklist** can be used to assist in documenting the privacy breach, but **don't wait** to compile all information requested above to report the breach.

Notice: *Remember that stopping/containing the breach and gathering the information should occur simultaneously with the reporting step, whenever possible.*

NM ATIP

1.3. Register the potential privacy breach, initiate an administrative review of the incident, and inform CFMWS Unit Security Supervisor (USS) of the possible security violation.

1.4. Immediately advise the CFMWS Vice-President Corporate Service (VP CorpSvcs), if the privacy breach is deemed to be "material". See Annex A: Definitions.

1.5. As required, and depending on the individuals affected, inform the ATIP coordinator of other government institutions, e.g. National Defence, Defence Research and Development Canada, Veterans Affairs, Defence Construction Canada, Royal Canadian Mounted Police.

VP CorpSvcs

1.6. Brief the Director General Morale and Welfare services (DGMWS) in a timely fashion when a "material" privacy breach is suspected and the expected timing for notifications to the Office of the Privacy Commissioner (OPC), Treasury Board Secretariat (TBS) and affected individuals.

Caution: *In responding to a privacy breach, be careful not to take steps that may exacerbate the existing breach or create a new one (e.g., disclosing additional personal information).*

STEP 2: FULL ASSESSMENT

NM ATIP

2.1. In collaboration with the OPI and the USS as required, assess potential risks to the affected individual(s) and to the CFMWS. The **PBRRA** is an essential tool to be used to assess the level of risks for all potential privacy breach incidents.

2.2. In collaboration with the USS, identify and recommend corrective actions and preventive measures to the OPI, including whether or not notification of the affected individual(s), the OPC and TBS is required.

USS

2.3. Initiate investigation of potential privacy breaches deemed to be of medium to high risk and report findings to the VP CorpSvcs and NM ATIP.

VP CorpSvcs

2.4. Organize a **breach response team (BRT)** in the case of a "material" privacy breach assessed as **high** or **severe**, as stated in the **PBRRA**, to ensure that a coordinated approach is taken to inform the DGMWS and to provide strategic direction and decision-making regarding the next steps (notifications, etc.). The BRT will be composed as follows:

- VP CorpSvcs;
- CIO;
- OPI Division Head;
- NM ATIP;
- USS; and,
- Director Communications and Marketing and the CF Legal Advisor (CFLA) as required.

2.5. If the privacy breach has or could become a matter of public interest, in consultation with the OPI, inform the CFMWS Director of Communications and Marketing to determine whether communications material may be required to answer questions from the public, media, etc. However, personal information should not be disclosed to the Director of Communications and Marketing as there is no need to know.

STEP 3: NOTIFICATION

USS

3.1. Determine whether notification should be delayed to ensure that any possible investigation (internal or external with law enforcement authorities is not compromised), and advise the NM ATIP and the OPI accordingly.

NM ATIP

3.2. Consider the following factors in deciding whether OPC and TBS should be notified of the privacy breach:

The personal information involved is sensitive.

There is a risk of identity theft or other harm, including pain and suffering or loss of reputation.

A large number of people are affected by the breach.

The information has not been fully recovered.

The organization requires assistance in responding to the privacy breach.

The breach is the result of a systemic problem, or a similar privacy breach has occurred before.

3.3. Notify the OPC and TBS in the case of a "material" privacy breach using the OPC *Privacy Act* breach report template.

NM ATIP is the single NPP liaison with the OPC.

OPI

(director or higher level)

3.4. Notify all affected individuals for a low risk privacy breach within 10 working days, by letter (first class recommended), if their personal information has been or has potentially been compromised through theft, loss or unauthorized disclosure. Notification to affected individual(s) should include:

- a general description of the incident, including the date and time;
- the source of the breach (whether CFMWS, a contractor or a party to a sharing agreement. Do not include name or other personal information of individual(s) who may have caused the breach;
- a list of the personal information elements that have been or may have been compromised;
- the measures taken or to be taken to retrieve the personal information, to stop/control the breach and prevent recurrence, and the timelines for mitigate measures, if not already underway, will be put into effect;
- advice to the individual to mitigate risks of identity theft or to deal with compromised personal information (e.g., SIN);
- the name and contact information of the OPI official with whom individuals can discuss the matter further or obtain assistance; and,
- a reference to the effect that the NM ATIP and USS have been notified of the nature of the breach as well as the OPC if applicable, and that the individual has a right of complaint to the OPC under the *Privacy Act*.

VP CorpSvcs

3.5. For medium to high risk privacy breach incidents, the decision to notify affected individuals will be made by the VP CorpSvcs in consultation with the OPI, NM ATIP, USS and CFLA as required.

NM ATIP

3.6. Also inform affected individuals of developments as the matter is further investigated and outstanding issues get resolved, if necessary.

Notice: *Care should be exercised in the notification process to not unduly alarm individuals, especially where the institution only suspects but cannot confirm that certain individuals have been affected by the breach.*

STEP 4: MITIGATION AND REMEDIATION

NM ATIP and USS	**4.1.** Work with OPI and other corporate stakeholders as required, to recommend corrective measures in order to address any issues identified in the **BPRRA** These may include: • training, education and awareness sessions; • review of internal policies or procedures; • improvements to infrastructure, processes and systems; • follow-up audits.
OPI (director or higher level)	**4.2. Determine other corrective measures** in conjunction with other sectors, such as Human Resources, IM/IT or the USS, depending on the seriousness of the breach and mitigating and aggravating factors. The consequences should be determined on a case-by-case basis.
	4.3. Develop an action plan in response to the recommendations, and ensure that the recommended measures are implemented. The plan should include prioritized action items with responsibilities and time lines. Do not to include any disciplinary actions that may have been or planned to be taken against an employee as a result of the privacy breach as this is protected personal information.
NM ATIP	**4.4.** Follow up with the OPI to ensure that a plan is developed and implemented to mitigate the risks identified during the investigation.
VP CorpSvcs	**4.5.** Provide an overall summary of the implementation of all privacy breach action plans to the CFMWS Executive Management Board on an annual basis.