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

2. 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.

PROTOCOLE SUR LES ATTEINTES À LA VIE PRIVÉE

DATE DE PUBLICATION : Septembre 2017
DATE DE RÉVISION : S.O.

APPLICATION

1. Le présent document est une ordonnance qui s'applique aux membres des Forces armées canadiennes et une directive qui s'applique aux employés du ministère de la Défense nationale (MDN) ainsi qu'au Personnel des fonds non publics (FNP), Forces canadiennes (FC) qui sont responsables de l'administration et de la prestation des activités, services et programmes des Biens non publics (BNP).

2. Il est entendu que ces derniers comprennent tous les BNP dévolus aux commandants d'unités, à d'autres éléments et au chef d'état-major de la défense (CEMD) en vertu des articles 38 à 41 de la *Loi sur la défense nationale*; toutes les activités du Personnel des FNP, FC, et l'ensemble des services et programmes des BNP, y compris les fonctions de diversification des modes de prestation des services qu'ils sont tenus d'exécuter et d'administrer dans le cadre de responsabilisation des BNP.

AUTORITÉ APPROBATRICE

2. Ce protocole est publié avec l'autorisation du directeur général – Services de bien-être et moral (DGSBM) en sa qualité de directeur général des BNP et chef de la direction (CDir) du Personnel des FNP, FC.

ENQUIRIES

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

DEMANDES DE RENSEIGNEMENTS

3. Les demandes de renseignements doivent être adressées au gestionnaire national du Programme d'accès à l'information et de protection des renseignements personnels (GN AIPRP) des Services de bien-être et moral des Forces canadiennes (SBMFC).

DEFINITIONS

4. Consult Annex A: Definitions.

DÉFINITIONS

4. Voir l'annexe A : Définitions.

POLICY OBJECTIVE

5. 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.

OBJECTIF DE LA POLITIQUE

5. La direction des SBMFC et le personnel à tous les niveaux doivent prendre toutes les mesures nécessaires pour s'assurer que la protection des renseignements personnels est une priorité élevée et atténuer le risque d'atteinte à la vie privée dans la mesure du possible. Sans une intervention rapide et appropriée à toute atteinte présumée ou réelle à la vie privée, l'organisation des SBMFC s'expose à des risques d'atteinte à sa réputation et de compromission des renseignements personnels.

PROCEDURES

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

PROCÉDURES

6. Voir l'annexe B : Mesures à prendre en cas d'atteinte à la vie privée.

MONITORING AND CONSEQUENCES

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

SURVEILLANCE ET CONSÉQUENCES

7. La surveillance et les conséquences définies dans la Politique sur les pratiques relatives à la vie privée des SBMFC s'appliquent au présent protocole.

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

RÉFÉRENCES

Lois et règlements :

a. *Loi sur la protection des renseignements personnels*

b. *Règlement sur la protection des renseignements personnels*

Publications du Conseil du Trésor :

a. Politique sur la sécurité du gouvernement

b. Politique sur la protection de la vie privée

c. Directive sur les pratiques relatives à la protection de la vie privée

d. Lignes directrices sur les atteintes à la vie privée

Politiques des SBMFC :

a. Politique sur le programme d'accès à l'information et de protection des renseignements personnels (AIPRP)

b. Politique sur les pratiques relatives à la protection de la vie privée

c. Ordonnances relatives à la sécurité

ANNEXES

Annexe A : Définitions

Annexe B : Procédures d'intervention d'atteinte à la vie privée

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.

ANNEXE A : DÉFINITIONS

Compromission : Divulgation, destruction, suppression, modification, utilisation ou interruption non autorisées de biens ou de renseignements, ou accès non autorisé à des renseignements.

Divulgation : Communication de renseignements personnels par une méthode quelconque (c'est-à-dire la transmission, la présentation d'une copie ou l'examen d'un document) à toute entité ou personne.

Besoin de connaître : Restriction de l’accès aux renseignements protégés ou classifiés aux personnes qui ont besoin d’accéder aux renseignements et de connaître ceux-ci pour exécuter leurs tâches.

Biens non publics : Les BNP sont définis à l’article 2 de la *Loi sur la défense nationale* (LDN) et comprennent tous les fonds et biens reçus pour les organismes des BNP ou administrés par eux ou par leur entremise, ainsi que tous les fonds et biens donnés aux membres des FAC ou par eux-mêmes pour leur bénéfice et leur bien-être collectifs.

Renseignements personnels : Renseignements, quels que soient leur forme et leurs supports, concernant un individu identifiable, tel que défini à l'article 3 de la *Loi sur la protection des renseignements personnels*. Par exemple, les renseignements relatifs à la race, la nationalité, l'origine ethnique, la religion, l'âge, l'état civil, l'adresse ou les études, ainsi que les antécédents médicaux, criminels, financiers ou d'emploi d'un individu. Les renseignements personnels comprennent aussi un numéro ou un symbole d'identification, comme le numéro d'assurance social, attribué à un individu.

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.

Vie privée : Droit d’un individu à son intimité et à être protégé contre toute intrusion injustifiée. Il s’agit aussi du droit d’une personne de garder le contrôle de ses renseignements personnels et de savoir à quelles fins ils sont utilisés, divulgués et où ils sont conservés.

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.

Atteinte à la vie privée : Création, collecte, utilisation, divulgation, conservation ou retrait inappropriée ou non autorisée de renseignements personnels, ou accès inapproprié ou non autorisé à de tels renseignements. Une atteinte à la vie privée peut survenir au sein d’une institution ou à l’extérieur, et être le résultat d'erreurs de bonne foi ou d'actes malveillants commis par des employés, des tiers, des partenaires ou des intrus.

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.

Renseignement ou bien protégé : Renseignement pouvant être visé par une exemption ou une disposition d'exclusion de la *Loi sur l'accès à l'information* ou de la *Loi sur la protection des renseignements personnels* parce que l'on peut raisonnablement s'attendre à ce que sa divulgation compromette l'intérêt non national.

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.

Atteinte substantielle à la vie privée : Atteinte à la vie privée qui concerne des renseignements personnels de nature délicate dont il serait raisonnable de penser qu’elle pourrait causer un dommage ou un préjudice grave à une personne ou qu’elle touche un grand nombre de personnes.

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.

Risque : Incertitude que peut engendrer l'exposition à des événements ou résultats non désirés. Il s'agit de l'expression de la probabilité et de l'incidence d'un événement susceptible de nuire à la réalisation des objectifs d'une organisation. La formule classique utilisée pour quantifier le risque combine l’importance des dommages et la probabilité, comme suit : risque = probabilité × répercussions.

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.

Accès non autorisé : Accès à des renseignements par une personne qui n’a pas fait l’objet d’une enquête de sécurité ou qui n’a pas un besoin de connaître.

Divulgation non autorisée : Divulgation interdite par la loi ou par des règlements, des directives ou des politiques ministériels ou gouvernementaux.

Incertitude : État, partiel ou total, du manque d’information nécessaire à la compréhension ou à la connaissance d’un événement, de ses conséquences ou de la probabilité qu’il se produise.

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

2.2. 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.

ANNEXE B : MESURES À PRENDRE EN CAS D'ATTEINTE À LA VIE PRIVÉE

Étape 1 : Découverte et signalement

Avis : *Dès qu'une atteinte à la vie privée réelle ou présumée est découverte, il faut prendre des mesures immédiates la réprimer et la signaler. On peut signaler une atteinte à la vie privée de différentes façons, mais on peut d'abord la déclarer par le biais d'une communication verbale. Il faut ensuite suspendre le processus ou l'activité qui est à l'origine de l'atteinte réelle ou présumée à la vie privée. Dans la mesure du possible, il faudrait réprimer et signaler simultanément l'atteinte à la vie privée.*

Bureau de première responsabilité (BPR)

1.1. Réprimer et confiner immédiatement l'atteinte à la vie privée, puis protéger les documents, les systèmes ou les sites Web compromis afin de prévenir tout autre vol ou toute autre perte, utilisation, divulgation, copie, modification ou élimination non autorisées de renseignements personnels, ou tout autre accès non autorisé à ceux-ci. Les stratégies de confinement proposées figurent à la **Liste de vérification en cas d'atteinte à la vie privée** (voir l'appendice 1 de l'annexe B).

1.2. Signaler sans tarder l'atteinte à la vie privée au gestionnaire national du programme d'accès à l'information et de protection des renseignements personnels (GN AIPRP), c.-à-d. dans un délai de 24 heures (1 jour ouvrable) après avoir été informé de toute atteinte à la vie privée réelle ou présumée.

Le signalement peut être effectué verbalement. Il faut ensuite remplir la **Partie 1 du Rapport d'atteinte à la vie privée et d'évaluation des risques** (voir l'appendice 2 de l'annexe B) et le transmettre par courriel à **ATIP.AIPRP@sbmfc.com** en tâchant d'y inclure les éléments suivants dans la mesure du possible :

- date à laquelle l'atteinte à la vie privée a été découverte et façon dont elle a été découverte;
- description de l'incident, dont la date et le lieu où il s'est produit;
- cause (si elle est connue);
- personnes/parties présumées avoir commis l'atteinte ou susceptibles d'avoir participé à l'atteinte (à l'interne ou à l'externe);
- description des données compromises;
- nombre de personnes touchées par l'atteinte à la vie privée;
- mesures prises pour réprimer ou confiner l'atteinte à la vie privée;
- résultats de la tentative de récupération des renseignements;

- vulnérabilité des Services de bien-être et moral des Forces canadiennes (SBMFC) et des personnes touchées;
- personnes avisées;
- mesures prises ou envisagées pour prévenir la récurrence;
- questions de sécurité étudiées; et,
- tout autre renseignement pertinent.

La **Liste de vérification en cas d'atteinte à la vie privée** peut servir à documenter l'atteinte à la vie privée, mais il ne faut **pas attendre** d'avoir recueilli tous les renseignements demandés ci-dessus pour signaler l'atteinte à la vie privée.

Rappel : *Dans la mesure du possible, il faut effectuer simultanément les étapes suivantes : réprimer et confiner l'attente à la vie privée, recueillir les renseignements pertinents et la signaler.*

GN AIPRP

1.3. Consigner l'atteinte possible à la vie privée, entreprendre un examen administratif de l'incident et informer le superviseur de la sécurité de l'unité (SSU) des SBMFC du manquement possible à la sécurité.

1.4. Informer immédiatement le vice-président des services généraux (VP SG) des SBMFC si l'atteinte à la vie privée est considérée comme « substantielle ». Voir l'annexe A : Définitions.

1.5. Au besoin, et selon le nombre de personnes touchées, informer le coordonnateur de l'AIPRP d'une autre institution fédérale, p. ex. la Défense nationale, Recherches et développement pour la défense Canada, Anciens Combattants Canada, Construction de défense Canada, la Gendarmerie royale du Canada.

VP SG

1.6. Informer en temps opportun le directeur général des Services de bien-être et morale (DGSBM) de toute atteinte à la vie privée « substantielle » présumée et du moment auquel l'information sera transmise au Commissariat à la protection de la vie privée (CPVP), au Secrétariat du Conseil du Trésor (SCT) et aux personnes touchées.

Mise en garde : *Au moment de prendre les mesures qui s'imposent en cas d'une atteinte à la vie privée, il faut prendre garde d'éviter toute démarche qui pourrait aggraver l'atteinte à la vie privée actuelle ou en créer une nouvelle (p. ex. divulgation de nouveaux renseignements personnels).*

Étape 2 : Évaluation complète

GN AIPRP

2.1. En collaboration avec le BPR et le SSU, s'il y a lieu, évaluer les risques possibles pour les personnes touchées et les SBMFC. Le **Rapport d'atteinte à la vie privée et d'évaluation des risques** est un outil essentiel pour évaluer le niveau de risque de tous les éventuels incidents d'atteinte à la vie privée.

GN AIPRP

2.2. En collaboration avec le SSU, déterminer les mesures correctives et préventives et les recommander au BPR, décider notamment s'il faut aviser ou non les personnes touchées et le CPVP.

SSU

2.3. Lancer une enquête sur les atteintes possibles à la vie privée présentant un risque moyen à élevé, et rendre compte des conclusions au VP SG et au GN AIPRP.

VP SG

2.4. Mettre sur pied une **équipe d'intervention en cas d'atteinte à la vie privée** dans l'éventualité d'atteinte substantielle à la vie privée considérée comme **importante** ou **grave**, conformément au **Rapport d'atteinte à la vie privée et d'évaluation des risques**, afin de s'assurer que l'organisation adopte une approche coordonnée relativement à la communication de renseignements au DGBSM, à savoir des conseils stratégiques sur la prise de décisions face aux prochaines étapes à suivre (notification, etc.). L'équipe sera composée des membres suivants :

- le VP SG;
- le chef des service d'information;
- le chef de division du BPR;
- le GN AIPRP;
- le superviseur de la sécurité de l'unité (SSU); et,
- le directeur des communications et du marketing ainsi que le conseiller juridiques des FC, au besoin.

BPR

2.5. Si l'atteinte à la vie privée devient un sujet d'intérêt public ou est susceptible de le devenir, en informer le directeur des communications et du marketing à la suite d'une consultation avec le VP SG afin d'évaluer le besoin de préparer des produits de communication pour répondre aux questions du public, des médias, etc. Cependant, il ne faut pas divulguer de renseignements personnels au directeur des communications et du marketing puisqu'il n'existe aucun besoin de connaître.

Étape 3 : Avis

SSU

3.1. Déterminer s'il est nécessaire de retarder la notification afin d'éviter de compromettre toute enquête possible (interne ou externe menée auprès des organismes d'application de la loi), et en informer le GN AIPRP et le BPR.

GN AIPRP

3.2. Prendre en considération les facteurs suivants lorsqu'il décide ou non d'informer le CPVP et le SCT de l'atteinte à la vie privée :

- les renseignements personnels en question sont sensibles;
- il existe un risque de vol d'identité ou d'autre préjudice, notamment la souffrance ou la perte de réputation;
- l'atteinte à la vie privée touche un grand nombre de personnes;
- la tentative pour récupérer la totalité de l'information a échoué;
- l'organisation a besoin d'aide pour gérer l'atteinte à la vie privée;
- l'atteinte à la vie privée découle d'un problème systémique ou une atteinte semblable s'est déjà produite.

3.3. Aviser le CPVP et le SCT en cas d'atteinte « substantielle » à la vie privée en suivant le modèle de rapport sur les atteintes en vertu de la *Loi sur la protection des renseignements personnels* du CPVP.

Seul le GN AIPRP assure la liaison entre les BNP et le CPVP.

BPR (directeur ou niveau supérieur)

3.4. Aviser toutes les personnes touchées en cas d'atteinte à la vie privée à faible risque au moyen d'une lettre (envoi prioritaire recommandé) dans un délai de 10 jours ouvrables si leurs renseignements personnels ont été ou peuvent avoir été compromis à la suite d'un vol, d'une perte ou d'une divulgation non autorisée. La notification aux personnes touchées devrait inclure l'information suivante :

- une description générale de l'incident, y compris la date et l'heure;
- la source de l'atteinte à la vie privée (qu'il s'agisse des SBMFC, d'un entrepreneur ou d'une partie à une entente d'échange de renseignements). Ne pas inclure le nom ou d'autres renseignements personnels des personnes qui pourraient avoir causé l'atteinte;
- une liste des renseignements personnels qui ont été ou qui pourraient avoir été compromis;

- les mesures prises ou envisagées pour récupérer les renseignements personnels, confiner l'atteinte à la vie privée et empêcher que l'atteinte se reproduise, et les délais dans lesquels les mesures d'atténuation seront mises en œuvre, si elles ne sont pas déjà en cours;
- des conseils sur les moyens d'atténuer les risques de vol d'identité ou sur les mesures à prendre lorsque les renseignements personnels ont été compromis (p. ex. numéro d'assurance sociale);
- le nom et les coordonnées d'un représentant du BPR à qui l'individu peut s'adresser pour discuter de la question ou pour obtenir de l'aide; et
- une mention précisant qu'on a informé le GN AIPRP, le SSU et le CPVP, le cas échéant, de la nature de l'atteinte à la vie privée et que la personne a le droit de porter plainte au CPVP en vertu de la *Loi sur la protection des renseignements personnels*.

VP SG

3.5. Pour ce qui est des incidents d'atteinte à la vie privée à risque moyen à élevé, la décision d'aviser les personnes touchées incombe au VP SG, en consultation avec le BPR, le GN AIPRP et le SSU, au besoin.

GN AIPRP

3.6. Tenir les personnes touchées au courant des progrès de l'enquête et du règlement des questions en suspens, au besoin.

Avis : *Au moment de la notification, il convient de veiller à ne pas alarmer inutilement les personnes visées par l'atteinte à la vie privée, particulièrement lorsque l'institution soupçonne, mais ne peut pas confirmer que certaines personnes pourraient avoir été touchées.*

Étape 4 : Atténuation et mesures correctives

GN AIPRP et SSU

4.1. Collaborer avec le BPR et d'autres intervenants ministériels, au besoin, afin de recommander des mesures correctives dans le but de résoudre tout problème ciblé dans le **Rapport d'atteinte à la vie privée et d'évaluation des risques**, notamment :

- la formation et la sensibilisation;
- un examen des politiques et des procédures internes;
- des améliorations à l'infrastructure, aux processus, aux systèmes;
- des vérifications de suivi.

BPR (directeur ou niveau supérieur)	**4.2. Définir d’autres mesures correctives** en collaboration avec d’autres secteurs comme les relations de travail, la GI/TI ou le SSU, en fonction de la gravité de l’atteinte à la vie privée et des facteurs atténuants ou aggravants. Les conséquences devraient être déterminées au cas par cas.
	4.3. Rédiger un plan d’action pour donner suite aux recommandations et s’assurer que les mesures recommandées sont mises en œuvre. Ce plan doit comprendre des mesures de suivi et des responsabilités établies par ordre de priorité et selon un calendrier. Ne pas inclure dans le plan d’action des mesures disciplinaires qui auraient été prises ou qu’on prévoit prendre envers un employé suite à une atteinte à la vie privée car ce sont des renseignements personnels protégés.
GN AIPRP	**4.4.** Effectuer un suivi auprès du BPR afin de s’assurer qu’un plan est élaboré et mis en œuvre pour atténuer les risques ciblés durant l’enquête.
VP SG	**4.5.** Présenter un aperçu général de la mise en œuvre de tous les plans d’action en cas d’atteinte à la vie privée au conseil de la haute direction des SBMFC sur une base annuelle.