Commissaire à la lutte contre la corruption Québec

UPAC PRÉVENIR VÉRIFIER ENQUÊTER

POLITIQUE DE GESTION

Nature	Administration	Bloc	1
Catégorie	Direction générale	Vol.	1.1
Sujet	**Sécurité de l'information**	No	DIR.GEN.-02
Dernière mise à jour :	2018-03-13	Révision prévue :	2023-03-13

1. Introduction

1.1 Contexte

1.1.1 Conformément à l'article 63.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, le Commissaire à la lutte contre la corruption (Commissaire) doit « prendre les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits ».

1.1.2 Par ailleurs, en vertu des articles 30 et 31 de la *Loi concernant la lutte contre la corruption*, le Commissaire veille « à ce que soient respectés les droits des personnes mises en cause à la suite d'une dénonciation, que ce soit ceux de la personne qui a effectué la dénonciation, ceux des témoins ou ceux des auteurs présumés des actes répréhensibles » et doit « prendre toutes les mesures nécessaires afin de s'assurer que l'anonymat de la personne qui a effectué une dénonciation soit préservé ».

1.2 Objectif

1.2.1 La présente politique de gestion vise à établir :

- 1.2.1.A une classification des documents dont les informations doivent être protégées par le Commissaire;
- 1.2.1.B le partage des rôles et responsabilités en matière de sécurité de l'information et;
- 1.2.1.C un cadre de référence au sujet de la transmission, de l'impression, de la conservation et de la destruction des documents classifiés et de ceux contenant des renseignements personnels.

1.3 Destinataire

1.3.1 Les membres du Commissaire, incluant le commissaire, les commissaires associés ainsi que tous les membres du personnel du Commissaire.

1.3.2 Les membres des équipes désignées par le gouvernement au sein de l'Unité permanente anticorruption (UPAC) dans la mesure où ces derniers utilisent des ressources appartenant au Commissaire, qu'il s'agisse des locaux, des documents ou de l'équipement, notamment roulant et informatique.

2. Définitions

2.1 Actif informationnel :

2.1.1 L'actif informationnel du Commissaire désigne l'ensemble des équipements informatiques : les ordinateurs, les applications informatiques et la documentation nécessaire à leur bon fonctionnement, les téléphones cellulaires, les appareils de poche, les logiciels et progiciels, les traitements informatiques et les données traitées par ordinateur.

2.2 Application web :

2.2.1 Logiciel de type client-serveur manipulable à l'aide d'un navigateur web. Il s'agit d'un site web dynamique, orienté vers une série de tâches précises, constituant une application en soi.

2.3 Collecticiel :

2.3.1 Logiciel qui permet à des utilisateurs reliés par un réseau de travailler en collaboration sur un projet.

2.4 Documents « classifiés » :

2.4.1 Les documents classifiés sont ceux qui, par leur nature, peuvent :

- 2.4.1.A entraver le déroulement d'une enquête en cours, à venir ou sujette à réouverture;
- 2.4.1.B avoir une incidence sur l'administration de la justice;

2.4.1.C causer un préjudice au Commissaire;
2.4.1.D mettre à risque l'intégrité physique d'une personne.

2.4.2 De plus, ils contiennent des renseignements pouvant faire l'objet de restriction en vertu de la *Loi sur l'accès aux documents des organismes publics, de la règle de la tierce partie et sur la protection des renseignements personnels.*

2.5 Documents « restreints » (protégés A) :

2.5.1 Tout document qui contient des informations révélant l'existence ou la nature d'une enquête, une méthode ou une technique d'enquête, et qui n'est pas susceptible d'entraver le déroulement d'une enquête en cours, à venir ou sujette à réouverture.

2.5.2 Par exemple : bilan tactique, bulletin d'information, circulaire contenant des informations tels que des numéros de plaques d'immatriculation, la date de naissance d'un individu, un endroit et une personne d'intérêt, un rapport de police, une liste du personnel de l'unité, etc.

2.6 Documents « confidentiels » (protégés B) :

2.6.1 Tout document qui contient des informations dont la divulgation est susceptible d'entraver le déroulement d'une enquête en cours, à venir ou sujette à réouverture, ou ayant une incidence sur l'administration de la justice et la sécurité publique.

2.6.2 Par exemple : état de situation par rapport à une opération en cours, profil d'un individu ou d'une organisation, description d'un *modus operandi* criminel, conversation d'écoute électronique, diagramme de relation, etc. Ces documents contiennent principalement des cibles potentielles.

2.7 Documents « secrets » (protégés C) :

2.7.1 Tout document qui contient des informations dont la divulgation serait susceptible de mettre en péril la sécurité d'une personne, de révéler l'identité d'une source confidentielle d'information ou de causer un préjudice à une personne qui est l'auteure du renseignement ou qui en est l'objet.

2.7.2 Par exemple : un rapport de dénonciation, une fiche d'inscription d'un informateur, le rapport de suivi des dossiers, etc.

2.8 Documents « non classifiés » (non protégés) :

2.8.1 Tout document qui n'est pas visé par l'une de ces côtes ne doit pas porter la mention « non classifié » ou « non protégé » puisque cette mention n'est pas un niveau officiel de classification. Un document qui ne porte pas de mention de protection est présumé être protégé et avoir été validé comme tel par l'expéditeur.

2.9 Documents du Commissaire :

2.9.1 Tout document, classifié ou non, produit par des membres du Commissaire ou par des membres des équipes désignées pour le compte du Commissaire.

2.10 Numéro de l'émetteur-récepteur :

2.10.1 Le numéro de l'émetteur-récepteur est un numéro de 5 chiffres attribué spécifiquement à un individu afin de préserver son identité en tant qu'émetteur ou récepteur d'un document.

2.11 Ordinateur :

2.11.1 Pour les fins de la présente politique, désigne les ordinateurs de bureau, les ordinateurs portatifs et les appareils de poche.

Nature	Administration	Bloc	1
Catégorie	Direction générale	Vol.	1.1
Sujet	**Sécurité de l'information**	No	DIR.GEN.-02
Dernière mise à jour :	2018-03-13	Révision prévue :	2023-03-13

2.12 Personnel autorisé :

2.12.1 Toute personne, qu'elle soit permanente, occasionnelle, étudiante, stagiaire ou contractuelle, dûment autorisée par son gestionnaire à utiliser un élément d'actif informationnel du Commissaire, pour la durée de son emploi ou pour une période déterminée.

2.13 Renseignement personnel :

2.13.1 Information à caractère non public concernant une personne physique et permettant de l'identifier, directement ou indirectement.

2.14 Support de stockage :

2.14.1 Le support de stockage est une mémoire de masse amovible servant à entreposer des données informatiques. Clé USB, disque dur, disque externe et autres.

2.15 Technologies de l'information :

2.15.1 Les technologies de l'information comprennent :

- 2.15.1.A le courrier électronique
- 2.15.1.B la messagerie SMS (Short Message System) ou texto
- 2.15.1.C l'accès à Internet
- 2.15.1.D les applications web
- 2.15.1.E l'Intranet

2.16 Virtual Private Network (VPN) :

2.16.1 Réseau étendu privé établi en créant des liaisons permanentes spécialisées entre réseaux internes à travers des réseaux publics afin de répondre aux besoins en partage des ressources des utilisateurs.

3. Principes généraux

3.1 Sécurisation des documents :

3.1.1 La personne à l'origine du document du Commissaire est responsable de déterminer si celui-ci doit être classifié et de lui attribuer le code approprié en fonction de la classification présentée à l'annexe A.

3.1.2 La classification, la transmission, l'impression, la conservation et la destruction des documents du Commissaire doivent respecter les exigences stipulées à l'annexe A de la présente politique.

3.2 Droit de propriété :

3.2.1 Les documents du Commissaire et leur contenu sont la propriété exclusive de ce dernier et ils ne peuvent pas être utilisés à d'autres fins que celles prévues à la *Loi concernant la lutte contre la corruption* en particulier et à l'administration de la justice en générale.

3.3 Droit de regard :

3.3.1 Le commissaire a un droit de regard sur l'utilisation des éléments d'actif informationnel par les membres du Commissaire, soit :

- 3.3.1.A avoir accès à toute information consignée sur l'équipement électronique au moyen du courriel, d'une application web ou des services d'Internet ou par tout autre moyen;
- 3.3.1.B procéder à une vérification particulière de l'utilisation qui est faite des actifs informationnels, d'un accès gouvernemental au courriel, à une application web ou aux services d'Internet pour des motifs opérationnels et procéder à l'analyse de leurs résultats.

Nature	Administration	Bloc	1
Catégorie	Direction générale	Vol.	1.1
Sujet	**Sécurité de l'information**	No	DIR.GEN.-02
Dernière mise à jour :	2018-03-13	Révision prévue :	2023-03-13

3.4 La règle de la tierce partie :

3.4.1 Aucun document, information ou renseignement du Commissaire communiqué à une organisation externe ne peut être utilisé, reproduit ou diffusé auprès d'une autre organisation sans l'autorisation du Commissaire, à moins qu'il s'agisse d'un poursuivant public tel que le Directeur des poursuites criminelles et pénales.

3.5 Le droit de savoir :

3.5.1 Les documents, les informations et les renseignements du Commissaire sont accessibles aux membres du Commissaire en fonction de l'autorisation dont ils disposent.

3.6 Le besoin de savoir :

3.6.1 Les membres du Commissaire limitent leur accès aux documents, aux informations et aux renseignements à ce qui est pertinent et nécessaire à la réalisation de leurs tâches et au respect de leurs responsabilités au sein de l'organisation.

4. Intervenants

4.1 Le commissaire :

4.1.1 veille au respect des principes et des règles de sécurité de l'information énoncés dans cette politique.

4.2 Le gestionnaire :

4.2.1 s'assure de l'application de la politique et des procédures s'y rattachant dans son unité administrative;
4.2.2 sensibilise son personnel aux dispositions de la politique et aux modalités de sa mise en œuvre;
4.2.3 détermine s'il est opportun d'accorder ou de retirer à un membre de son unité administrative le droit d'utiliser un élément de l'actif informationnel;
4.2.4 s'assure que les éléments d'actifs opérationnels sont utilisés en conformité avec cette politique de gestion.

4.3 Le membre du Commissaire ou d'une équipe désignée :

4.3.1 se conforme à la présente politique et des procédures s'y rattachant;
4.3.2 conserve, transmet et détruit tous les documents classifiés ou contenant des renseignements personnels selon les modalités de l'annexe A;
4.3.3 signale immédiatement à son supérieur le vol, la perte ou l'oubli d'un document classifié;
4.3.4 signale immédiatement à l'agence émettrice le vol, la perte ou l'oubli d'un document classifié;
4.3.5 recueille, auprès de l'agence émettrice, l'autorisation de partager, de diffuser ou d'utiliser tout document ou information dont elle est l'auteure ou le propriétaire;
4.3.6 signale immédiatement à son supérieur le vol, la perte ou l'oubli d'un élément d'actif informationnel;
4.3.7 établit immédiatement avec son gestionnaire l'importance de l'information perdue ou volée;
4.3.8 utilise un accès gouvernemental au courriel, au message *SMS*, à une application web et aux services d'Internet à des fins pertinentes à la réalisation de ses fonctions;
4.3.9 s'engage, à moins d'autorisation de son gestionnaire, à ne pas transporter ou entreposer des documents classifiés, sous toutes ses formes, à l'extérieur des bureaux sécurisés du Commissaire.

4.4 Le technicien en informatique :

4.4.1 s'assure de l'application de la politique envers les éléments d'actifs informationnels sous sa responsabilité;
4.4.2 signale immédiatement au commissaire toute dérogation dans l'utilisation des actifs informationnels du Commissaire;

Nature	Administration		Bloc	1
Catégorie	Direction générale		Vol.	1.1
Sujet	**Sécurité de l'information**		No	DIR.GEN.-02
Dernière mise à jour :	**2018-03-13**	**Révision prévue :**	**2023-03-13**	

4.4.3 maintien à jour l'inventaire de tous les éléments d'actifs informationnels sous sa responsabilité ou en prêt de service;
4.4.4 configure adéquatement les éléments d'actifs informationnels afin que ces derniers conservent les standards de sécurité du Ministère de la Sécurité publique (MSP).

4.5 La Direction des technologies de l'information du MSP :
4.5.1 fournit les logiciels de courriel, de collecticiel et d'accès à Internet, les entretient et en assure la sécurité;
4.5.2 s'assure que les postes de travail (ordinateurs de table ou portables) sont équipés d'un logiciel antivirus à jour;
4.5.3 vérifie, sur demande du commissaire, la conformité de l'utilisation des boîtes de messageries et de l'Internet;
4.5.4 évalue régulièrement les vulnérabilités et les risques susceptibles de nuire aux ressources technologiques constituant le réseau étendu ministériel.

4.6 Le responsable des applications web :
4.6.1 Sur demande du commissaire associé aux vérifications administratives :
4.6.1.A journalise toute activité se produisant sur ces applications;
4.6.1.B restreint les accès de tout utilisateur et de toute application sans préavis.

5. Procédures

5.1 Vous devez consulter la section « Documents officiels » de l'intranet de l'UPAC afin de trouver les procédures et les formulaires qui sont liés à cette politique de gestion.

6. Cadre légal et règlementaire

6.1 La Loi sur la police;
6.2 La Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels;
6.3 La Loi sur la fonction publique;
6.4 La législation en matière de droits d'auteur;
6.5 La Loi concernant la lutte contre la corruption.

7. Autres informations pertinentes

8. Approbation

Robert Lafrenière
Commissaire à la lutte contre la corruption

Date 2018/03/16