Sécurité de l'information

Recommandation du groupe de travail portant sur la sensibilisation à la sécurité de l'information

Ministère de la Sécurité publique

Version : 0.9

Mise à jour : 2014-04-10

Québec

HISTORIQUE DES CHANGEMENTS

Version	Date	Description	Auteur
0.6	2013-03-11	Ébauche originale	Samuel Morin
0.7	2013-06-19	Mise à jour du document	Samuel Morin
0.8	2014-02-12	Mise à jour du document	Samuel Morin
0.9	2014-04-10	Intégration des commentaires des différents participants.	Samuel Morin

TABLE DES MATIÈRES

1. CONTEXTE

Les normes internationales et les bonnes pratiques en sécurité de l'information reconnaissent la sensibilisation du personnel comme un levier stratégique et puissant pour améliorer la gestion des risques informationnels ainsi que le niveau global de sécurité d'une organisation. La formation et la sensibilisation du personnel sont des voies à privilégier afin de permettre à chacun de prendre conscience des enjeux, des risques et des bonnes pratiques à adopter en sécurité de l'information. Elles permettent d'agir simultanément sur plusieurs risques liés à la sécurité de l'information.

En janvier 2014, l'adoption de la nouvelle directive sur la sécurité de l'information gouvernementale visait à établir une vision commune de la sécurité de l'information au sein des ministères et organismes gouvernementaux. Cette directive comporte une section « Obligations générales des organismes publics en matière de sécurité de l'information » qui impose à chacun des ministères de « *définir et mettre en place un programme formel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.* »

Bien que l'objet principal de la Directive porte sur la protection de l'information gouvernementale, celle-ci ne fait pas abstraction des exigences de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, auxquelles sont soumis tous les organismes publics. La loi exige non seulement de prendre les mesures de sécurité propres à assurer la protection des renseignements personnels, mais elle prévoit également toute une série de restrictions pouvant s'appliquer aux divers documents détenus par un organisme public et qui, de ce fait, leur confère, dans bien des cas, un caractère confidentiel.

Tant dans les normes que dans les pratiques exemplaires en sécurité de l'information, il est reconnu que la gestion de la sécurité doit être soutenue par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle, d'où le besoin de sensibiliser le personnel du ministère de la Sécurité publique à la sécurité de l'information.

Plus précisément, la sensibilisation fera connaître :

- Les risques et leurs conséquences pour le ministère ou l'organisme;
- Les mesures de sécurité en place;
- Les responsabilités de chacun face à la sécurité de l'information numérique et des échanges électroniques;
- Les comportements à encourager et les gestes à proscrire;
- Les procédures à suivre en cas d'atteinte, réelle ou appréhendée, à la sécurité.

2. CONSULTATION

Ce programme a été élaboré par la DTI en collaboration avec un groupe de travail formé des intervenants suivants :

- Monsieur André Senécal, ComDP
- Monsieur Claude Crête, DTI
- Monsieur Pierre Avon, UPAC
- Madame Sandra Langevin, RACJ
- Monsieur Samuel Morin, DTI
- Monsieur Benoit Mathieu, DRH
- Monsieur Ismail Daoudi, DVIEI
- Madame Chantale Bergevin, DGSC
- Monsieur Jérôme Gagnon, DGAP

3. OBJECTIFS

La sécurité de l'information est devenue un enjeu majeur, principalement, en raison de l'utilisation des échanges accélérés d'information à l'aide de moyens technologiques hautement sophistiqués qui facilitent la diffusion et l'accès. Ces moyens sont de plus en plus exposés aux attaques informatiques provenant de partout.

Le personnel ministériel produit, reçoit, traite, consulte, conserve, transmet et élimine de l'information pour laquelle des règles de sécurité doivent être mises en place et respectées par chacun des employés, quelle que soit sa fonction dans l'organisation. Le contexte dans lequel l'information est traitée, stockée et communiquée a beaucoup évolué dans les dernières décennies.

Dans ce contexte, un programme de base ciblant l'ensemble des employés et visant une introduction aux bonnes pratiques en matière de sécurité de l'information est donc tout à fait approprié. De plus, tout en s'inscrivant dans le cadre de la mise en œuvre de la Loi sur la gouvernance et la gestion des ressources informationnelles (LGGRI), la mise en place d'un programme formel de sensibilisation à la sécurité de l'information, appuyé par les plus hautes autorités du ministère répond à plusieurs autres exigences :

- Il constitue une étape de mise en œuvre de la directive sur la sécurité de l'information gouvernementale;
- Il permet de concrétiser l'une des actions inscrites dans le plan déposé à la Direction de la vérification interne;
- Il soutient l'appropriation des bonnes pratiques en la matière en contribuant à développer une culture de sécurité de l'information chez son personnel;
- Il facilite l'intégration de la sécurité de l'information dans la gestion et le pilotage d'orientation des actifs ministériels et des actifs d'intérêt commun.

La mise en œuvre d'un tel programme permet aussi d'atteindre plusieurs objectifs de résultat, notamment que le personnel :

- Intègre dans ses activités quotidiennes une appréciation du risque liée à la valeur de l'information qu'il utilise et adopte les comportements et les actions appropriés pour en assurer la protection;
- Connaisse les enjeux et les risques liés à l'utilisation des RI et applique les mesures les plus appropriées à son contexte;
- Se responsabilise en matière de sécurité de l'information par la connaissance des bonnes pratiques en la matière.

Enfin, le programme contribuera à satisfaire les exigences contenues dans la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et le Règlement sur la diffusion de l'information et la protection des renseignements personnels qui confient au sous-ministre la responsabilité de veiller à la sensibilisation et à la formation de membres du personnel de direction sur les obligations et les pratiques en matière d'accès à l'information et de protection des renseignements personnels.

4. STRATÉGIE DE COMMUNICATION

La stratégie proposée est celle d'une communication évolutive, en fonction des connaissances du personnel, afin que ceux-ci adhèrent aux valeurs organisationnelles et aux orientations internes en matière de sécurité de l'information en plus de prendre conscience de l'importance de protéger les informations confidentielles et stratégiques.

Le comité de travail a statué que la formation devra être obligatoire pour tous les employés du MSP et de ses organismes. Les capsules de formation seront diffusées dès la première année et les vidéos seront utilisés l'année suivante. Le comité a aussi statué qu'il faudrait adapter la formation à certains cadres d'emploi (ex. : garde du corps) et bien cibler les thèmes qui les concernent. L'adaptation pourrait aussi se faire au niveau de la diffusion de la formation. En effet, certains cadres d'emploi particulier pourraient être formés en groupe en classe avec animation. Cette stratégie permettrait de former les employés qui n'ont pas accès quotidien à un ordinateur.

De plus, le comité a décidé de décentraliser le suivi en nommant un responsable par chacune des unités administratives. Le MSP devra aussi prévoir la gestion du taux de roulement et devra déterminer les conséquences pour les retardataires qui ne suivent pas les formations.

5. PUBLICS CIBLES

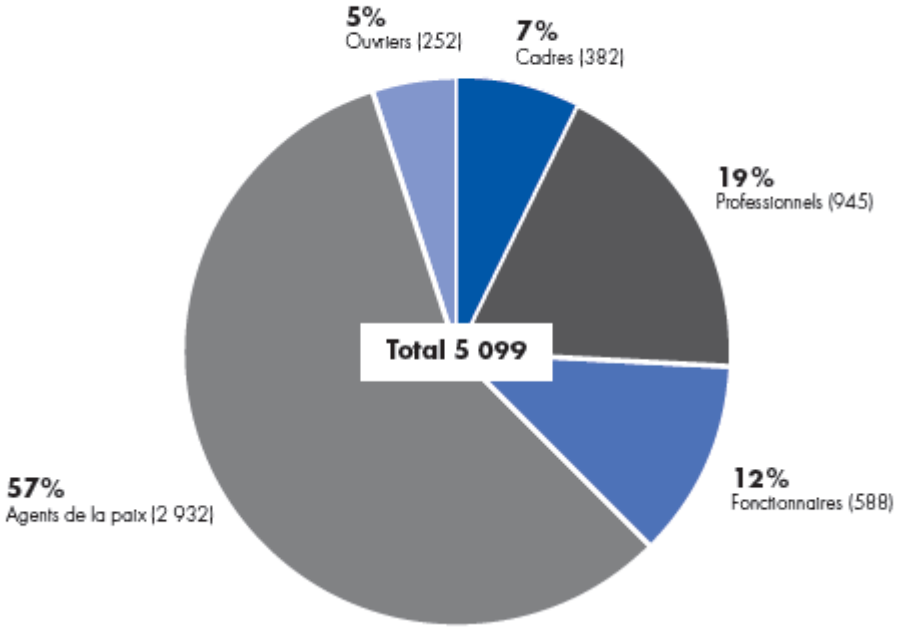
Les gestionnaires du ministère de la Sécurité publique, le personnel ou tout autre employé (prêt de service, étudiant, stagiaire) qui utilisent un équipement informatique du ministère ou qui ont accès à de l'information, quelle que soit la forme de celle-ci.

5.1. Ministère de la Sécurité publique (MSP)

Tableau 8 : Répartition de l'effectif total autorisé 2012-2013 (exprimé en ETC)

Programmes	2012-2013	2011-2012	Variation
	Autorisé[1]	Autorisé[2]	(%)
1. Sécurité, prévention et gestion interne			
Direction et services de soutien à la gestion	275	275	0,0
Services correctionnels	3 825	3 441	11,2
Expertises judiciaires	133	122	9,0
Affaires policières et sécurité-protection	469	436	7,6
Sécurité civile et sécurité incendie	257	179	43,6
Éléments de gestion centrale	0[3]	0[3]	S/O
Sous-total – Ministère	4 959	4 453	11,4
2. Sûreté du Québec	7 713[4]	7 399[4]	4,2
Total	12 672	11 852	6,9

Graphique 2 : Total des employés du ministère (à l'exception de la SQ)



Direction ou Organisme	Nombre d'employés
Ministère de la Sécurité publique (MSP)	5099
Bureau du coroner (BC)	124
Comité de déontologie policière (CQLC)	38
Commissaire à la lutte contre la corruption (UPAC)	42
Commission québécoise des libérations conditionnelles (CQLC)	90
École nationale de police (ENPQ)	368
École nationale des pompiers	16
Commissaire à la déontologie policière (ComDP) (Exclue)	72
Régie des alcools, des courses et des jeux (RACJ) (Exclue)	338
Total	**5777**

6. RÉSULTATS ATTENDUS

- Faire en sorte que tous les gestionnaires du MSP comprennent le rôle prépondérant qu'ils ont à jouer auprès de leurs employés afin que ceux-ci intègrent les bonnes pratiques en matière de sécurité de l'information;

- S'assurer que 80 % des utilisateurs du MSP ont pris connaissance des risques et des conséquences inhérents à la gestion de l'information et à l'utilisation des ressources informationnelles face aux comportements et aux attitudes à adopter pour assurer en tout temps et en tout lieu la protection de l'information;

- Rehausser de 50 % les compétences de la moitié du personnel du MSP dans l'application des règles d'usage et des pratiques recommandées en matière de sécurité de l'information et de protection des renseignements personnels.

7. MOYENS DE COMMUNICATION

Dans le but de développer une véritable culture organisationnelle intégrant les principes de sécurité de l'information et faire face aux changements constants et rapides dans les ressources informationnelles, le programme de sensibilisation et de formation des employés s'échelonnera sur une période de trois ans. Il comprendra des activités de formation, d'information et de promotion pour la clientèle visée.

8. ACTIVITÉS DE FORMATION

8.1. Formation en ligne

Considérant le fait qu'il n'y a pas eu de sensibilisation à la sécurité de l'information depuis plusieurs années, et tenant compte de la diversité des thèmes à aborder, une approche basée sur l'auto apprentissage en ligne a été retenue. Cette approche offre les avantages suivants :

- Une démarche flexible et souple sur le plan des horaires d'apprentissage;
- Facile d'accès et aucun frais relatif aux déplacements;
- Les nouveaux employés pourront bénéficier, dans leur programme d'accueil, de la même formation.

Découpées en courtes capsules thématiques, les cours en ligne ont l'avantage d'uniformiser les connaissances de l'ensemble du personnel sur les pratiques à adopter et expliquer, lors des années subséquentes, les politiques et directives du ministère. Les thèmes abordés sont énumérés dans l'annexe A.

Des bulletins d'information et des vidéos en lien avec les thèmes des capsules seront aussi utilisés pour rappeler les points principaux à retenir.

8.2. Vidéos de sensibilisation

Le ministère de la Sécurité publique achètera 18 vidéos de rappel destinées à tous les employés. Ces séquences véhiculent des messages importants sur les meilleures pratiques en matière de sécurité. Les vidéos seront diffusés en même temps que les capsules de formation.

8.3. Formation en classe

Le ministère de la Sécurité publique envisage adapter sa formation à certains corps d'emploi. En effet, certaines formations pourraient être données en groupe avec animation. Cette stratégie permettrait de former les employés qui n'ont pas un accès quotidien à un ordinateur.

9. ACTIVITÉS D'INFORMATION ET DE PROMOTION

9.1. Affichage

Le ministère de la Sécurité publique achètera les droits de 18 affiches. Une affiche pour chaque thème abordé pendant la campagne de sensibilisation.

Une fois les affiches achetées, nous pouvons en imprimer le nombre que nous désirons. Les affiches seront ensuite affichées à tous les étages du siège social et dans tous les établissements du ministère.

9.2. Bulletins de nouvelles

Le ministère de la Sécurité publique achètera 18 bulletins de nouvelles en lien avec la sécurité de l'information. Les bulletins seront envoyés à chaque employé et diffusés sur l'intranet. Les bulletins seront en liens avec les thèmes abordés pendant la campagne de sensibilisation.

Ces différents bulletins adresseront les préoccupations du ministère au regard de la sécurité de l'information en résumant les bonnes pratiques et les conséquences que pourrait avoir le non-respect des directives.

9.3. Messages à l'ouverture

Dans le but de rappeler les différentes consignes en sécurité de l'information des messages seront affichés lors de l'ouverture de la session des utilisateurs.

Le ministère de la Sécurité publique obtiendra gratuitement 60 messages intranet(conseils) avec l'achat des capsules de sensibilisation. Ses messages pourront être affichés lors de l'ouverture de la session des utilisateurs et être envoyés par courriel pour s'assurer que les employés en prennent connaissance.

9.4. Messages d'attente lors des appels au Technocentre

Le Technocentre enregistrera des messages en liens avec la sécurité de l'information pour diffuser lorsque les employés attendent au téléphone pour recevoir du dépannage. Ces messages seront un excellent moyen de communiquer les directives en matière de sécurité de l'information.

9.5. Promotion (nouvelles Intranet, courriel)

La formation en ligne fera l'objet d'une promotion par l'intermédiaire du personnel d'encadrement et de la Direction des ressources humaines (DRH), en collaboration avec la Direction des communications (DCOM). Ainsi, des nouvelles sur l'intranet et des invitations par courriel seront les outils de communication privilégiés.

9.6. Bandeau électronique

Afin d'associer les nouvelles dans l'intranet et les courriels envoyés à la démarche de sensibilisation à la sécurité de l'information, il faudra développer visuel commun pour tous les outils de communication.

9.7. Slogan commun

Dans le même ordre d'idées, un slogan commun à la majorité des outils de communication devra être utilisé. Il viendra en appui au visuel développé.

9.8. Semaine thématique

Dans le but de mobiliser le personnel autour de l'enjeu de la sécurité de l'information, une semaine thématique viendra soutenir les efforts de promotion. Pour les années subséquentes, la semaine thématique ainsi créée aura l'avantage de permettre un retour périodique sur un aspect particulier de la sécurité de l'information.

Lors du lancement de la première semaine thématique, les autorités du ministère auront l'occasion de faire connaître leurs priorités et d'insister sur l'importance de protéger les informations auxquelles chaque membre du personnel a accès dans le cadre de ses fonctions. Les capsules animées seront lancées lors de cette semaine.

10. ÉCHÉANCIER

Mai 2014	
Approbation de la campagne	− Informer la Direction et les gestionnaires de la tenue d'une campagne ministérielle de sécurité de l'information.
Mai 2014	
Début des préparatifs de la campagne	− Signature de l'entente avec Terranova − Formation de l'administrateur de la campagne. − Recensement des utilisateurs à former par unité administrative. − Mettre à jour la section Sécurité de l'information dans l'intranet. − Conception de la signature visuelle et des outils de communication. − Formation des employés du Service à la clientèle pour le soutien téléphonique et technique. − Configuration des rapports.
Mai 2014	
Annonce de la campagne et distribution de la trousse aux gestionnaires.	− Outiller les gestionnaires afin qu'ils soient en mesure d'informer leur personnel sur la formation et la campagne à venir.
Fin Mai 2014	
Hameçonnage éthique	− Évaluer l'état de situation actuel du ministère − Permettre de prendre conscience de l'ampleur du problème
Début Juin 2014	
Annonce de la Semaine à venir sur la sécurité de l'information et distribution du jeu-questionnaire initial	− Jeu-questionnaire auprès du personnel: « Mesurez vos connaissances en matière de sécurité de l'information ». − Distribution d'une affiche «Ne pas déranger, je suis en formation» au personnel pour que celui-ci puisse le poser devant son bureau durant sa formation.
23 au 27 Juin 2014	
Semaine de la sécurité de l'information et mise en ligne de la formation	− Début de la formation en ligne pour l'ensemble du personnel − Diffusion du programme d'activités (conférences, concours, etc.) − Affichage
23 Juin au 17 Juillet 2014	
Formation en ligne	− Période pour compléter la formation et/ou l'examen démontrant l'acquisition des connaissances.
Août 2014	
Rétroaction	− État de situation de la participation
23 Juin 2015	
Début de la deuxième année : Semaine de la sécurité de l'information et	− Début de la diffusion des vidéos de sensibilisation en ligne pour l'ensemble du personnel − Mettre à jour la section Sécurité de l'information dans l'intranet.

mise en ligne de la formation	− Diffusion du programme d'activités (conférences, concours, etc.) − Affichage
En continu	
Publication de nouvelles et de rappels dans l'intranet	− Nouvelles ponctuelles sur l'intranet redirigeant vers la section web sur les bonnes pratiques ou vers de nouvelles directives ou politiques en matière de sécurité de l'information.
En continu	
Sensibilisation de tous les nouveaux employés par l'utilisation des capsules de formation	− Un feuillet d'information sera ajouté dans la pochette d'accueil les invitant à suivre la formation en ligne − Un code d'accès pour la formation en ligne sera transmis à tout nouvel employé par le service à la clientèle de la DTI lors de son inscription aux services informatiques.

ANNEXE A : THÈMES

1. **Introduction à la sécurité de l'information (7 capsules)**
    - Introduction à la sécurité de l'information
    - La gestion des menaces et des risques
    - La propriété intellectuelle
    - La création d'un mot de passe efficace
    - Le courrier électronique
    - Les pourriels
    - Les codes malicieux
2. **La protection physique (5 capsules)**
    - La protection physique
    - Le principe du bureau propre
    - Le contrôle d'accès
    - L'ingénierie sociale
    - Les équipements personnels au travail
3. **La protection des informations sensibles (7 capsules)**
    - La classification de l'information
    - La gestion de l'information
    - Les communications externes
    - La protection des renseignements personnels
    - La protection des cartes de crédit
    - La destruction des renseignements et des actifs sensibles
    - Le vol d'identité
4. **L'internet et le travail à distance (6 capsules)**
    - La confidentialité sur le Web
    - Le bon usage d'Internet au travail
    - Les réseaux sociaux
    - Les utilisateurs nomades
    - La sécurité des téléphones intelligents
    - La sécurité dans les nuages (Cloud computing)

ANNEXE B : BUDGET

Activités	Description	Date début	Date fin	Année 1	Année 2	Année 3
Cours de sensibilisation en ligne pour les utilisateurs	21 sujets + évaluations	2014-06-01	2017-06-01	31 250$	0 $	0 $
	Personnalisation du contenu pour le MSP	2014-06-01	2017-06-01	5 000$	0 $	0 $
	Frais de maintenance annuelle (2015-2016)	2014-06-01	2017-06-01	0$	6250$	6250$
	Hébergement de plateformes LMS (incertitude)	2014-06-01	2017-06-01	6 000$	6000 $	6000$
Affiches de sensibilisation	Achat des droits de 18 affiches	2014-06-01	2017-06-01	3 695$	0 $	0 $
Impression des affiches de sensibilisation	Impression de 540 affiches de dimension 16 X 20 pouces sur du papier satin	2014-06-01	2017-06-01	2 457$	0 $	0 $
Bulletins de nouvelles de sensibilisation	18 bulletins de nouvelles	2014-06-01	2017-06-01	4 100$	0 $	0 $
Vidéos de sensibilisation	18 vidéos	2014-06-01	2017-06-01	0$	8400 $	0 $
Fonds d'écran de sensibilisation	18 fonds d'écran	2014-06-01	2017-06-01	Gratuit (valeur de 3 695$)	0 $	0 $
Messages intranet (conseil)	60 messages conseil (envoyer à chaque utilisateur par courriel)	2014-06-01	2017-06-01	Gratuit (valeur de 1 200$)	0 $	0 $
Total des investissements en activité de sensibilisation avec hébergement du fournisseur (2014 à 2017)				52 502$	20 650 $	12 250 $
Total des investissements en activité de sensibilisation avec hébergement au MSP (2014 à 2017)				46 502 $	14 650$	6250$

PROJET

Sécurité publique
Québec