



Liste de vérification des politiques – Responsabilités du dirigeant principal de la sécurité (DPS)

Les présentes lignes directrices visent à aider les DPS à s’acquitter de leurs responsabilités telles qu’énoncées dans la [Politique sur la sécurité du gouvernement](#) (PSG). La Politique et ses instruments d’appui s’appliquent¹ aux ministères tels que définis à l’article 2 et aux entités figurant aux annexes IV et V de la [Loi sur la gestion des finances publiques](#) (LGFP).

La PSG de 2019 exige que les administrateurs généraux (AG) désignent un DPS², dont le rôle est de fournir des conseils stratégiques et un leadership de haut niveau à l’échelle du ministère, ainsi que d’assurer la coordination et la surveillance des activités de gestion de la sécurité, y compris les huit mesures de sécurité³.

La section 4.1 de la [Directive sur la gestion de la sécurité](#) (DGS) décrit les responsabilités des DPS en ce qui a trait à l’appui des responsabilités de l’AG en vertu de la PSG. À titre de conseiller stratégique principal sur les risques en matière de sécurité⁴, le DPS s’acquitte de ses responsabilités en matière de sécurité en menant les activités suivantes :

Plan de sécurité ministériel (PSM)
<u>Responsabilités de l’administrateur général</u> ➤ Approuver le PSM (un examen annuel est nécessaire) qui établit des stratégies pour répondre aux exigences ministérielles en matière de sécurité (y compris le traitement des huit mesures de sécurité de la PSG) qui tiennent compte des priorités de sécurité pangouvernementales et y contribuent. <u>Responsabilités des DPS</u> ☐ Diriger la fonction de sécurité ministérielle en définissant, en documentant, en mettant en œuvre, en évaluant, en surveillant et en maintenant les exigences, les pratiques et les mesures de sécurité. ➤ Veiller à ce que les huit mesures de sécurité et les pratiques connexes soient en place, surveillées et maintenues. ☐ Superviser l’élaboration, la mise en œuvre et la tenue à jour du PSM, en collaboration avec d’autres hauts fonctionnaires et intervenants. ➤ Veiller à ce que le PSM : • soit à jour et approuvé annuellement par l’AG (cycle de trois ans); • offre une vue intégrée des menaces, des risques et des exigences du ministère en matière de sécurité, y compris les activités d’atténuation; • comprenne des stratégies, des priorités, des responsabilités et des échéanciers pour le maintien, le renforcement, le suivi et l’amélioration continue des pratiques de sécurité en ce qui concerne les huit mesures de sécurité. ☐ Rendre compte à l’AG des progrès réalisés dans l’atteinte des priorités définies dans le PSM. ➤ Rendre compte annuellement à l’AG concernant les priorités. ➤ Recommander des changements aux pratiques de sécurité, aux mesures de sécurité et aux priorités du ministère (au besoin).

¹ À moins d’en être exclus aux termes de lois, de règlements ou de décrets particuliers.

² À titre de rappel, les DPS délégués doivent envoyer leur lettre de désignation (dûment signée par l’AG) et leurs coordonnées à la Division de la Politique sur la sécurité du SCT à l’adresse SEC@tbs-sct.gc.ca dans les 4 semaines suivant leur désignation.

³ Les huit mesures de sécurité sont définies dans la [Politique sur la sécurité du gouvernement – Annexe A : Mesures de sécurité](#).

⁴ Le DPS est responsable des décisions en matière de gestion des risques de sécurité connexes.

Ressources

- [Nouveau modèle de plan de sécurité ministériel \(PSM\)](#)
- [Page GCpédia de la PSG](#)

Filtrage de sécurité

Responsabilités de l'administrateur général

- Veiller à ce qu'une décision de refuser, de révoquer ou de suspendre une cote ou une autorisation de sécurité (secret, très secret, accès au site) ne soit pas déléguée.
- Examiner tout risque résiduel du contrôle de sécurité dépassant la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité.
- Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes.

Responsabilités des DPS

☐ **Veiller à ce que les filtrages de sécurité soient effectués de façon efficace, rigoureuse, uniforme et juste afin qu'ils offrent une assurance raisonnable et continue que des personnes dignes de confiance protègent l'information et les actifs du gouvernement et qu'elles s'acquittent de leurs fonctions de façon fiable et afin d'assurer la transférabilité des filtrages de sécurité entre les ministères.**

- Le filtrage de sécurité doit être effectué conformément à la [Norme sur le filtrage de sécurité](#).

☐ **Surveiller l'établissement de processus à l'échelle du ministère afin d'évaluer et de documenter les mesures concernant les risques résiduels liés au filtrage de sécurité pour les programmes et les services du ministère et les ressources à l'appui.**

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

Gouvernance

Responsabilités de l'administrateur général

- Assurer l'établissement de la gouvernance de la sécurité ministérielle pour les mesures de sécurité, y compris les responsabilités relatives aux mesures de sécurité et les pouvoirs décisionnels en matière de gestion des risques pour la sécurité.

Responsabilités des DPS

☐ **Surveiller l'élaboration, la mise en œuvre et le maintien de la gouvernance interne de la sécurité ministérielle, qui définit les responsabilités relatives aux fonctions de sécurité et les pouvoirs décisionnels en matière de gestion des risques pour la sécurité.**

☐ **Veiller à ce que l'AG soit représenté dans les comités de gouvernance de la sécurité du GC en participant à l'établissement de l'orientation de gestion de la sécurité à l'échelle du gouvernement.**

- Cela comprend le Comité sur la sécurité et la préparation du gouvernement du Canada (CSPGC), le Comité sur les mesures de sécurité intégrées du gouvernement du Canada⁵ (CMSI GC) et le Comité des sous-ministres adjoints sur la sécurité (CS SMA), le cas échéant.

⁵ La Politique offre la souplesse d'établir une gouvernance de la sécurité du ministère qui convient au contexte ministériel. La portée des responsabilités d'un DPS dans un petit ministère ou organisme (PMO) est la même que celle dans un ministère plus vaste, bien que l'échelle puisse être différente.

Sécurité de la technologie de l'information
<u>Responsabilités de l'administrateur général</u> ➤ Examiner tout risque résiduel de sécurité informatique qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité. ➤ Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées sont prises pour régler ces problèmes. <u>Responsabilités des DPS</u> ☐ Veiller à ce que les exigences, les pratiques et les mesures relatives à la sécurité de la technologie de l'information soient définies, documentées, mises en œuvre, évaluées, surveillées et tenues à jour à chaque étape du cycle de vie des systèmes d'information, ce qui permet de fournir une assurance raisonnable que les systèmes d'information sont en mesure de protéger adéquatement l'information, sont utilisés de façon acceptable et appuient les programmes, les activités et les services gouvernementaux. ☐ Surveiller l'établissement de processus à l'échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels liés à la sécurité de la technologie de l'information pour les programmes et les services du ministère et les ressources à l'appui. ➤ Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

Sécurité matérielle
<u>Responsabilités de l'administrateur général</u> ➤ Examiner tout risque résiduel de sécurité matérielle dépassant la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité. ➤ Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes. <u>Responsabilités des DPS</u> ☐ Veiller à ce que les exigences, les pratiques et les mesures liées à la sécurité matérielle soient définies, documentées, mises en œuvre, évaluées, surveillées et tenues à jour à toutes les étapes du cycle de vie de la gestion des biens immobiliers et du matériel, ce qui permet de fournir une assurance raisonnable que les particuliers, l'information et les actifs sont adéquatement protégés, appuyant ainsi la prestation de programmes, de services et d'activités du gouvernement. ➤ Définir et documenter les pratiques ministérielles en matière de sécurité pour la réalisation d'évaluations et les autorisations relatives à la sécurité des installations et des inspections de sécurité des installations, y compris celles qui ont des exigences de sécurité plus élevées. ☐ Surveiller l'établissement de processus à l'échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels liés à la sécurité matérielle pour les programmes et les services du ministère et les ressources à l'appui. ➤ Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

Gestion de la continuité des activités
<u>Responsabilités de l'administrateur général</u> ➤ Examiner tout risque résiduel lié à la gestion de la continuité des activités qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité. ➤ Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes. <u>Responsabilités des DPS</u>

☐ **Veiller à ce que la gestion de la continuité des activités soit menée de manière systématique et complète, qu'elle fournisse une assurance raisonnable qu'en cas de perturbation, le ministère pourra garantir un niveau acceptable de prestation des services et des activités critiques, et qu'il sera en mesure de reprendre rapidement les autres services et activités.**

- Les ministères et les organismes doivent effectuer des essais réguliers⁶ (c'est-à-dire, tous les deux ans) des plans de continuité des activités pour assurer un état de préparation acceptable, y compris l'essai des systèmes fonctionnels⁷.

☐ **Surveiller l'établissement de processus à l'échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels liés à la gestion de la continuité des activités pour les programmes et les services du ministère et les ressources à l'appui.**

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

Sécurité de la gestion des renseignements

Responsabilités de l'administrateur général

- Examiner tout risque résiduel lié à la sécurité de la gestion des renseignements qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité.
- Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes.

Responsabilités des DPS

☐ **Veiller à ce que les exigences, les pratiques et les mesures de contrôle en matière de sécurité de la gestion des renseignements soient définies, documentées, mises en œuvre, évaluées, surveillées et tenues à jour à toutes les étapes du cycle de vie de l'information afin de fournir une assurance raisonnable que l'information est protégée adéquatement de façon à respecter les obligations juridiques et autres et à équilibrer le risque de préjudice et de menace avec le coût de l'application des mesures de protection.**

☐ **Surveiller l'établissement de processus à l'échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels liés à la sécurité de la gestion des renseignements pour les programmes et les services du ministère et les ressources à l'appui.**

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

Exigences de sécurité liées aux contrats et autres ententes

Responsabilités de l'administrateur général

- Établir des ententes écrites avec d'autres organisations lorsqu'elles reçoivent des services de sécurité⁸.
- Examiner tout risque résiduel de sécurité associé aux contrats et autres ententes qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité.
- Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes.

⁶ Les exercices comprennent les arbres de communication (appel direct, communication ou réponse par courriel ou message texte), un accès à un site et une capacité fonctionnelle de replis, la capacité d'accéder à distance aux applications essentielles et la capacité de PCA du fournisseur, entre autres. Les exercices peuvent comprendre des ateliers, des simulations sur maquettes, des exercices d'entraînement ou des simulations.

⁷ Les essais fonctionnels comprennent des exercices, des exercices fonctionnels et des exercices à l'échelle réelle.

⁸ Cela comprend les services liés au filtrage de sécurité, à la sécurité de la TI, à la sécurité matérielle, à la gestion de la continuité des activités, à la sécurité de la gestion de l'information, à la sécurité des contrats, à la sécurité de l'immeuble de base, à la gestion des événements, à la sensibilisation et à la formation.

Responsabilités des DPS

☐ Veiller à ce que les exigences de sécurité liées aux contrats⁹ et autres ententes soient déterminées et documentées, et que les mesures de sécurité connexes soient mises en œuvre et surveillées à chaque étape du processus d’octroi de contrats ou d’établissement d’ententes, afin de fournir une assurance raisonnable que l’information, les particuliers, les actifs et les services liés au contrat ou à l’entente sont protégés de façon adéquate.

☐ Surveiller l’établissement de processus à l’échelle du ministère afin d’évaluer et de documenter les mesures concernant les risques résiduels associées à la sécurité liées aux contrats pour les programmes et les services du ministère et les ressources à l’appui.

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

☐ Vérifier que des accords écrits sont en place lorsque l’organisation fournit des services de sécurité à un autre ministère ou organisme ou en reçoit de ce ministère ou organisme.

- S’applique uniquement aux ententes interministérielles¹⁰ qui relèvent du paragraphe 29.2 de la *Loi sur la gestion des finances publiques* (LGFP), et aux ententes conclues avec des sociétés d’État, d’autres ordres de gouvernements, le secteur privé et d’autres entités non régies par la PSG.
- S’applique aux marchés portant sur la production ou la livraison de biens ou de services, et à toute autre entente concernant le partage de biens ou de renseignements de nature délicate avec des organisations¹¹ ou des personnes qui ne sont pas régies par la PSG.

Gestion des événements liés à la sécurité

Responsabilités de l’administrateur général

- Veiller à ce que les incidents de sécurité et autres événements liés à la sécurité fassent l’objet d’une évaluation et d’une enquête, et qu’ils soient documentés, traités et signalés à l’autorité adéquate ainsi qu’aux intervenants touchés.
- Répondre aux directives, aux conseils et aux demandes d’information provenant du Secrétariat du Conseil du Trésor du Canada et du Bureau du Conseil privé concernant les événements liés à la sécurité qui nécessitent une intervention immédiate ou des mesures coordonnées dans l’ensemble du gouvernement.
- Examiner tout risque résiduel lié à la gestion des événements de sécurité qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité.
- Mener une enquête et prendre des mesures lorsque surviennent d’importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes.

Responsabilités des DPS

☐ Veiller à ce que des pratiques relatives à la gestion des événements liés à la sécurité soient définies, documentées, mises en œuvre et tenues à jour afin d’assurer la surveillance; répondre et signaler les menaces, les vulnérabilités, les incidents et d’autres événements liés à la sécurité, en plus de veiller à ce que de telles activités soient coordonnées de façon efficace au sein du ministère, avec les partenaires et dans l’ensemble du gouvernement, ce qui permet de gérer les incidences possibles, d’appuyer la prise de décisions et de permettre la mettre en œuvre des mesures correctives.

☐ Surveiller l’établissement de processus à l’échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels associées à la gestion

⁹ La sécurité nationale doit être prise en compte tout au long du processus d’octroi de contrats ou d’établissement d’ententes (c’est-à-dire, les clauses de sécurité nationale dans les ententes de contribution et la chaîne d’approvisionnement). Pour les contrats et autres arrangements avec les fournisseurs, la Liste de vérification des exigences relatives à la sécurité (LVERS) peut aider à déterminer les exigences relatives à la sécurité nationale.

¹⁰ L’entité doit avoir le pouvoir de conclure de tels ententes ou arrangements.

¹¹ Comprend les autres ordres de gouvernement et les partenaires universitaires ou scientifiques.

des événements liés à la sécurité pour les programmes et les services du ministère et les ressources à l'appui.

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes et les limitations, et elles doivent être testées et validées.

□ Superviser l'établissement de processus panministériels pour surveiller et assurer une réponse coordonnée aux menaces, aux vulnérabilités, aux incidents de sécurité et à d'autres événements relatifs à la sécurité propres aux ministères, ainsi que leur signalement.

- Les processus doivent comprendre la détermination des mesures à prendre pour remédier aux lacunes.
- Les incidents de sécurité et autres événements de sécurité importants doivent être signalés au Secrétariat du Conseil du Trésor du Canada par courriel à SEC@tbs-sct.gc.ca, de façon cyclique ou sur demande, aux fins de la surveillance de la Politique à l'échelle du gouvernement.
- Les atteintes importantes à la vie privée doivent être signalées aux **deux** organisations suivantes :
 - le Commissariat à la protection de la vie privée du Canada par courriel à notification@priv.gc.ca;
 - le Secrétariat du Conseil du Trésor du Canada par courriel à SEC@tbs-sct.gc.ca.

□ Veiller à ce que tous les enjeux importants liés au respect de la Politique, aux activités criminelles potentielles, aux préoccupations en matière de sécurité nationale et aux autres enjeux de sécurité fassent l'objet d'une évaluation et d'une enquête, soient documentés, traités et signalés à l'AG.

- Au besoin, les problèmes doivent être signalés aux autorités policières compétentes et/ou aux organismes de sécurité et de renseignement (voir l'annexe I : Norme sur le signalement des incidents de sécurité), et aux intervenants concernés.
- Au besoin, coopérer à toute enquête criminelle ou autre qui en résulterait.

□ Collaborer avec d'autres hauts fonctionnaires et d'autres intervenants pour répondre aux demandes orientations, aux conseils et aux demandes d'information provenant du Secrétariat du Conseil du Trésor du Canada à titre d'employeur (y compris le Bureau du dirigeant principal des ressources humaines), du Bureau du Conseil privé et du Centre des opérations du gouvernement (COG) concernant des événements liés à la sécurité qui nécessitent une intervention immédiate ou coordonnée dans l'ensemble du gouvernement.

- Les incidents et événements de sécurité doivent être signalés sans délai au Centre des opérations du gouvernement (COG) par téléphone au 613-991-7000 ou par courriel à GOC-COG@ps-sp.gc.ca et au Bureau du dirigeant principal de la sécurité du BCP par téléphone au 613 960-4000 ou par courriel à CMC-CGC@pco-bcp.gc.ca.
- Les incidents de cybersécurité et d'autres événements de sécurité liés à la technologie de l'information (TI) doivent être signalés conformément au [Plan de gestion des événements de cybersécurité du gouvernement du Canada](#) (PGEC GC).

Sensibilisation et la formation en matière de sécurité

Responsabilités de l'administrateur général

- Examiner tout risque résiduel lié à la sensibilisation et la formation en matière de sécurité qui dépasse la portée des pouvoirs décisionnels établis en matière de gestion des risques pour la sécurité.
- Mener une enquête et prendre des mesures lorsque surviennent d'importants problèmes de conformité à la Politique, ainsi que de veiller à ce que les mesures correctives appropriées soient prises pour régler ces problèmes.

Responsabilités des DPS

□ Veiller à ce que la sensibilisation et la formation en matière de sécurité soient offertes de façon systématique et complète afin de veiller à ce que chaque personne connaisse ses responsabilités en matière de sécurité, maintienne les connaissances et les

compétences nécessaires afin de s’acquitter adéquatement de ses fonctions et d’offrir une assurance raisonnable que les personnes ne compromettent pas délibérément la sécurité et qu’ils comprennent les conséquences potentielles de ne pas s’acquitter de leurs responsabilités en matière de sécurité.

☐ Surveiller l’établissement de processus à l’échelle du ministère pour évaluer et documenter les mesures prises au sujet des risques résiduels liés à la sensibilisation et formation en matière de sécurité pour les programmes et les services du ministère et les ressources à l’appui.

- Des mesures correctives doivent être mises en œuvre pour remédier aux lacunes. Les limitations doivent être testées et validées.

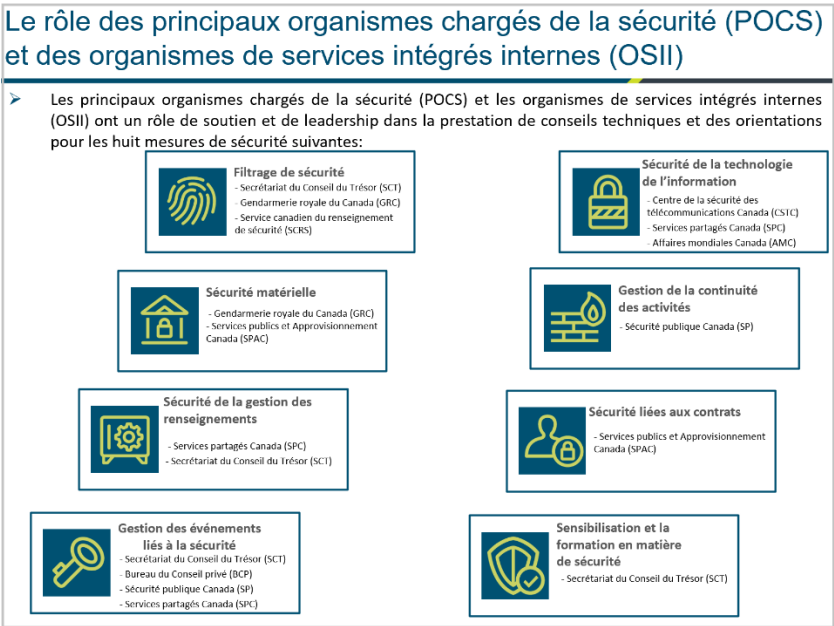
Annexe A – Principaux organismes chargés de la sécurité et organismes de services internes intégrés

La [Politique sur la sécurité du gouvernement](#) (PSG) identifie les organisations gouvernementales qui ont un rôle clé à jouer pour assurer l'exécution en toute confiance des programmes et la prestation des services du gouvernement du Canada (GC) par une gestion efficace de la sécurité à l'appui de la protection de l'information, des personnes et des actifs du GC.

Ces principaux organismes chargés de la sécurité (POCS) et/ou organismes de services intégrés internes¹² (OSII) contribuent à la réalisation des objectifs de la PSG :

- ❖ en participant à la gouvernance pangouvernementale de la Politique sur la sécurité pour contribuer à établir les orientations stratégiques et les priorités qui cadrent avec les objectifs en matière de sécurité nationale et les autres priorités du gouvernement;
- ❖ en fournissant des conseils et en élaborant des directives techniques et opérationnelles pour aider les ministères à mettre en œuvre les politiques;
- ❖ en fournissant des services internes intégrés sécurisés à d'autres ministères du GC, dispensés à l'échelle du gouvernement (les OSII identifiés seulement);
- ❖ en consultant le Secrétariat du Conseil du Trésor du Canada (SCT), Affaires mondiales Canada (AMC) et d'autres POCS et intervenants pertinents au moment d'établir des accords internationaux, traités ou d'autres instruments qui pourraient avoir des incidences sur les pratiques en matière de gestion de la sécurité à l'échelle du gouvernement;
- ❖ en participant à l'analyse des menaces, des vulnérabilités, des risques et des événements liés à la sécurité, et en transmettant les conclusions aux intervenants pertinents;
- ❖ en offrant de l'expertise pour appuyer la création des programmes de sensibilisation et de formation en matière de sécurité du GC.

Figure 1 : Rôles des POCS et OSII



Consultez la [section 5](#) de la PSG pour obtenir des renseignements supplémentaires sur les responsabilités des POCS et OSII.

Coordonnées des POCS et OSII

Veuillez consulter la [liste des personnes-ressources en matière de sécurité du GC](#) pour consulter les coordonnées.

¹² Ministère ou organisation qui offre des services internes intégrés à d'autres ministères du gouvernement du Canada. Cela comprend les principaux organismes chargés de la sécurité qui fournissent des services de sécurité à l'échelle du gouvernement.

Annexe B – Renseignements, ressources et outils supplémentaires sur la Politique

Le [site Web](#)¹³ GCpédia de la [Politique sur la sécurité du gouvernement](#) (PSG) fournit aux spécialistes fonctionnels de la sécurité des renseignements, des ressources et des outils liés à la PSG.

Orientation sur les mesures de sécurité

Pour chacune des huit mesures de sécurité de la PSG, le Secrétariat du Conseil du Trésor du Canada (SCT), les principaux organismes chargés de la sécurité (POCS) et les organismes de services internes intégrés (OSII) partagent des conseils, des orientations et des ressources pour aider les ministères et organismes à mettre en œuvre ces mesures.

Tableau 1 – Orientations et outils stratégiques ¹⁴			
Filtrage de sécurité Annexe A : Procédures obligatoires de filtrage de sécurité Outil d'analyse des postes (OAP) Trousse d'outils du filtrage de sécurité Fichier « type » et transférabilité du filtrage de sécurité 2020 Fichier de renseignements sur le filtrage de sécurité du personnel POCS/OSII : SCT, GRC, SCRS Lignes directrices du SCT Lignes directrices de la GRC Lignes directrices du SCRS	Sécurité matérielle Annexe C : Procédures obligatoires relatives aux mesures de sécurité matérielle Méthodologie harmonisée d'évaluation des menaces et des risques (EMR) Manuel de la sécurité des contrats Guide pour la préparation d'un énoncé de sécurité matérielle POCS/OSII : GRC, SPAC Lignes directrices de la GRC Lignes directrices de SPAC	Sécurité de la technologie de l'information Annexe B : Procédures obligatoires relatives aux mesures de sécurité de la technologie de l'information Orientation sur la gestion des rustines Orientation sur l'utilisation des signatures électroniques POCS/OSII : CST, AMC, SPC Lignes directrices du CST Lignes directrices du CCC Lignes directrices du CCSSN Lignes directrices d'AMC Lignes directrices de SPC	Sécurité la gestion de l'information Annexe E : Procédures obligatoires relatives aux mesures de sécurité de la gestion de l'information Directive sur la gestion de la sécurité – annexe J : Norme sur la catégorisation de sécurité SCT –Modèle actuel de catégorisation de la sécurité du GC POCS/OSII : SPC, SCT Lignes directrices du SCT
Gestion de la continuité des activités Annexe D : Procédures	Exigences de sécurité associées aux contrats et autres arrangements	Gestion des événements liés à la sécurité Annexe G : Procédures	Sensibilisation et formation relatives à la sécurité

¹³ À titre de rappel, GCpédia est un outil d'application interne essentiel au partage des connaissances pour les employés fédéraux et n'est accessible que par le biais du réseau ministériel ou de la connexion RPV.

¹⁴ Un accès et/ou un compte peuvent être nécessaires pour accéder aux ressources disponibles sur GCpédia et GCconnex figurant dans le tableau.

obligatoires de gestion de la continuité des activités – mesures de contrôle • Guide pour l'élaboration d'un programme de gestion de la continuité des activités POCS/OSII : SP • Lignes directrices de SP	• Annexe F : Procédures obligatoires pour la sécurité de l'octroi de contrats et autres arrangements – mesures de contrôle • Listes de vérification des exigences relatives à la sécurité (LVERS) • Exigences de sécurité des contrats du gouvernement du Canada • Services en direct de sécurité industrielle POCS/OSII : SPAC • Lignes directrices de SPAC	obligatoires relatives aux mesures de sécurité dans la gestion des événements • Annexe I : Norme sur le signalement des événements de sécurité • Protocole d'échange d'information sur les incidents marquants (décembre 2019) • Plan de gestion des événements de cybersécurité du gouvernement du Canada (PGEC GC) 2019 • BCP – Guide opérationnel sur les niveaux de préparation de sécurité (mars 2020) POCS/OSII : SP, BCP, SPC et SCT. • Lignes directrices de SP • Lignes directrices du SCT • Lignes directrices du BCP	• Annexe H : Procédures obligatoires de formation et de sensibilisation en matière de sécurité – mesures de contrôle • GTSS – Ressources de sensibilisation à la sécurité • L'Outil d'apprentissage des employés sur la sensibilisation à la sécurité POCS/OSII : SCT • Lignes directrices du SCT
---	--	--	---

Facilitateurs stratégiques clés

En vertu de la Politique, Bibliothèque et Archives Canada (BAC) et l'École de la fonction publique du Canada (ÉFPC) sont désignés comme des facilitateurs stratégiques clés appuyant les priorités et les objectifs en matière de sécurité à l'échelle du gouvernement. Il est important de souligner que la collaboration continue avec les organismes centraux, les POCS, les OSII, les responsables des politiques et la collectivité fonctionnelle de la sécurité, ainsi que leur participation active à la gouvernance des politiques sur la sécurité, à titre de facilitateurs, renforcent la gestion de la sécurité du gouvernement du Canada (GC).

Le SCT continue de collaborer avec l'ÉFPC afin de veiller à ce que les ministères reçoivent un apprentissage et une formation appropriée, et avec de petits organismes pour élaborer des lignes directrices et des outils simplifiés adaptés à leurs besoins. Cela garantit que les pratiques de gestion de la sécurité au sein des ministères, avec les partenaires et à l'échelle du gouvernement, sont appuyées par des orientations, des outils et des opportunités d'apprentissage et de formation modernes et efficaces.

Forums de la collectivité et gouvernance

Les forums de la collectivité offrent aux dirigeants principaux de la sécurité¹⁵ (DPS) et aux spécialistes fonctionnels de la sécurité la possibilité de communiquer, de collaborer et d'échanger de l'information. Ceux-ci incluent le Sommet annuel sur la sécurité du GC, des forums de sécurité du GC d'une demi-journée¹⁶ tenus trois fois par année et d'autres activités et événements de mobilisation communautaire qui encouragent le réseautage et le partage des pratiques exemplaires dans l'ensemble de la collectivité de la sécurité. Le SCT continue de collaborer avec

15 Les ordres du jour des réunions précédentes du Forum de la sécurité du GC et les documents connexes sont disponibles sur [GCpédia](#).

les DPS, les POCS et les OSII par l'entremise de comités de gouvernance du GC sur la sécurité établis afin de renforcer et de maintenir des pratiques de gestion de la sécurité mûres, et d'assurer le leadership, la surveillance et des forums afin de traiter les questions et les préoccupations émergentes en matière de sécurité.

La gouvernance de la sécurité du GC comprend actuellement les comités suivants :

- **Comité des sous-ministres adjoints sur la sécurité (CS SMA) :** Coprésidé par le SCT et le Bureau du Conseil privé (BCP), le comité offre une orientation stratégique et assure un leadership en ce qui concerne l'élaboration, la mise en œuvre et l'évaluation continues de la Politique sur la sécurité du gouvernement et les activités de préparation opérationnelle. Il appuie une approche intégrée entre les responsables de sécurité principaux, les fournisseurs de services organisationnels internes, les organismes centraux et les ministères. Des renseignements supplémentaires, y compris le mandat, se trouvent dans la [page du groupe](#) GCconnex du CS SMA (statut de membre requis).
- **Comité sur la sécurité et la préparation du gouvernement du Canada (CSPGC) :** Coprésidé par le SCT et le Bureau du Conseil privé (BCP), le comité agit à titre d'organisme consultatif auprès du Comité des sous-ministres adjoints sur la sécurité (CS SMA) pour la mise en œuvre de l'ensemble des politiques sur la sécurité du GC et des activités connexes de préparation. Des renseignements supplémentaires, y compris le mandat, se trouvent dans la [page du groupe](#) GCconnex du CSPGC (statut de membre requis).
- **Comité sur les mesures de sécurité intégrées du gouvernement du Canada (CMSI GC) :** Présidé par le SCT, le comité offre une tribune pour la surveillance, l'échange de lignes directrices et de conseils à titre de POCS/OSII afin d'assurer une approche cohérente et intégrée au moyen de stratégies d'atténuation des risques, en éclairant la Politique sur la sécurité (en remplissant le rôle de POCS ou d'OSII), en assurant la continuité des opérations et en mobilisant les communautés de pratique connexes. Des renseignements supplémentaires, y compris le mandat, se trouvent dans la [page du groupe](#) GCconnex du CMSIGC (statut de membre requis).
- [Sommet sur la sécurité du gouvernement du Canada \(annuel\)](#)

En outre, des questions ponctuelles liées à la politique de sécurité, à la préparation et à la gestion des urgences font l'objet de discussions et sont considérées comme pertinentes par les comités identifiés au tableau 2.

Tableau 2 – Gouvernance pour la politique sur la sécurité du GC, la préparation et la gestion des urgences

Domaine	Nom du comité
Politiques	• Comité consultatif sur la gestion de la fonction publique (CCGFP) • Comité des sous-ministres sur les priorités et la planification intégrées (SM CPPI) • Comité des sous-ministres adjoints sur les services et les priorités intégrées (SMA SPI)
État de préparation	• Comité sur la sécurité nationale des sous-ministres
Urgence	• Comité de gestion des urgences des sous-ministres (CGU SM)* • Cellule de crise des sous-ministres adjoints (CC SMA)* • Comité de gestion des urgences des directeurs généraux (CGU DG)* • Comité d'intervention des directeurs généraux (CGI DG)*

*Appuie la réponse du GC à la pandémie de COVID-19 dans le cadre du Plan fédéral d'intervention d'urgence (PFIU).

Coordonnées

Bibliothèques et Archives Canada (BAC)

- Pour de plus amples renseignements, veuillez visiter le [site](#) de la Gestion de l'information et disposition des documents du gouvernement.

École de la fonction publique du Canada (ÉFPC)

- Pour obtenir de plus amples renseignements sur le contenu d'apprentissage offert à la collectivité de la sécurité, veuillez visiter la [page](#) des spécialistes fonctionnels de la sécurité sur GCcampus.

Centre canadien pour la cybersécurité (CCC)

- Pour de plus amples renseignements, vous pouvez visiter le [site](#) du Centre pour la cybersécurité ou communiquer avec le Centre canadien pour la cybersécurité (CCC), par courriel, à contact@cyber.gc.ca ou, par téléphone, au 1-833-292-3788.

Service canadien du renseignement de sécurité (SCRS)

- Centre intégré d'évaluation des menaces (CIEM)
 - Vous pouvez contacter le CIEM pour toute préoccupation liée à l'évaluation de la menace terroriste pour les Canadiens et les intérêts canadiens à l'étranger, à l'adresse courriel ITAC1@smtp.gc.ca.
- Sécurité nationale
 - Vous pouvez contacter le Service canadien du renseignement de sécurité (SCRS) pour toute question relative à la sécurité nationale, par téléphone, au 613-993-9620.
- Le Bureau de liaison gouvernementale (BLG) est le principal point de contact de la Direction de l'évaluation du renseignement (DER) du Service. Les dirigeants principaux de la sécurité (DPS) peuvent envoyer un courriel à glo@smtp.gc.ca pour les motifs suivants :
 - les demandes de renseignements du Service, y compris les évaluations de la menace;
 - les demandes de séances d'information sur le renseignement (à noter qu'ils n'offrent pas de séances d'information sur les voyages);
 - les demandes d'ajout à la liste de diffusion pour les produits d'évaluation du Service;
 - toute rétroaction sur les produits d'évaluation du Service.

Centre du droit du travail et de l'emploi (CDTE)

- Le Centre du droit du travail et de l'emploi (CDTE) est chargé de fournir des conseils juridiques en matière de droit du travail et de l'emploi directement aux ministères et organismes clients. Veuillez consulter la liste des contacts du CDTE pour trouver les coordonnées d'un représentant ou vous pouvez joindre Christian.Demers@justice.gc.ca ou Nancy.Paradis@tbs-sct.gc.ca.

Nota : Les demandes de conseils juridiques concernant les habilitations secrètes et les révocations doivent être adressées à Justice Canada.

Opération INTERSECT

- Vous pouvez contacter l'équipe des opérations d'INTERSECT pour toute question relative à la préparation et à la gestion des situations d'urgence multi juridictionnelles, à l'adresse Intersect@ottawapolice.ca.

Sécurité publique (SP)

- Centre de gestion de la continuité et de la résilience (CGCR)
 - Vous pouvez communiquer avec le Centre de gestion de la continuité et de la résilience (CGCR) de la SP pour obtenir des conseils et des orientations sur l'élaboration et la mise en œuvre d'un programme de CGCR par courriel à crcm-cgcr@ps-sp.gc.ca ou par téléphone au 613- 949-6522.
- Centre des opérations du gouvernement (COG)
 - Vous pouvez communiquer avec le Centre des opérations du gouvernement (COG) de la SP pour toute question relative à la gestion des événements de sécurité par courriel à goc-cog@ps-sp.gc.ca ou par téléphone au 613-991-7000.

- Sécurité nationale et politique de cybersécurité
 - Pour de plus amples informations, veuillez consulter le [site](#) de la Sécurité nationale de la SP ou communiquer avec le Programme de coopération en matière de cybersécurité par courriel à CSCP-PCCS@ps-sp.gc.ca.

Services publics et Approvisionnement Canada (SPAC)

- Sécurité de l'immeuble de la base
 - Vous pouvez communiquer avec la Sécurité de l'immeuble de la base de SPAC pour toute question relative à la sécurité physique et à la sécurité des immeubles de la base par courriel à TPSGC.securiteimmeublebase-basebuildingsecurity.PWGSC@tpsgc-pwgsc.gc.ca.
- Programme de sécurité des contrats (PSC)
 - Vous pouvez communiquer avec le Programme de sécurité des contrats de SPAC pour toute demande de renseignements concernant les exigences de sécurité des contrats et les filtrages de sécurité par courriel à ssi-iss@tpsgc-pwgsc.gc.ca, par téléphone au 613-948-4176 ou au numéro sans frais au 1-866-368-4646. L'information est également disponible sur la page Web du [centre de service à la clientèle du Programme de sécurité des contrats](#).
- Programme des marchandises contrôlées (PMC)
 - Vous pouvez communiquer avec le SPAC pour toute demande de renseignements concernant les marchandises contrôlées qui impliquent des entrepreneurs par courriel à dmc-cgd@tpsgc-pwgsc.gc.ca, par téléphone au 613-948-4176 ou au numéro sans frais au 1-866-368-4646.

Gendarmerie royale du Canada (GRC)

- Services canadiens d'identification criminelle en temps réel (SCICTR)
 - Vous pouvez communiquer avec les SCICTR de la GRC pour toute question relative à la vérification des casiers judiciaires par courriel, à CCRTIS-SCICTR@rcmp-grc.gc.ca
- Centre national des opérations (CNO)
 - Vous pouvez communiquer avec le CNO de la GRC pour toute question relative à la sécurité nationale par courriel, à SIR-SIS@rcmp-grc.gc.ca ou par téléphone, au 613-993-4460.
- Section du filtrage sécuritaire (SFS)
 - Vous pouvez communiquer avec la SFS de la GRC pour toute question relative à la vérification des antécédents criminels par courriel, à SIBSAdmin-SFSAdmin@rcmp-grc.gc.ca.

Bureau du Conseil privé (BCP)

- Cellule de gestion de crise (CGC)
 - Vous pouvez communiquer avec la CGC du BCP pour toute demande de renseignements relative à la gestion d'un événement de sécurité (y compris les menaces à l'encontre de ministres et du premier ministre), pour tout problème de sécurité nationale ou en cas de changement de votre niveau de préparation en matière de sécurité par courriel à CMC-CGC@pco-bcp.gc.ca ou par téléphone au 613-960-4000.
- Centre d'excellence en sécurité (CEeS)
 - Vous pouvez communiquer avec le CEeS pour tout soutien dont vous pourriez avoir besoin, du recrutement à la professionnalisation et aux questions opérationnelles allant de filtrages de sécurité complexes à l'exercice de vos plans d'urgence par courriel à SCoE-CEeS-info@pco-bcp.gc.ca.
 - [Jeunes professionnels de la sécurité : GCcollab](#)
 - [Centre d'excellence en sécurité : GCcollab](#)

Secrétariat du Conseil du Trésor (SCT)

- Division de la cybersécurité
 - Pour de plus amples renseignements sur la cybersécurité au sein du gouvernement du Canada, veuillez consulter la [page GCéchange sur la cybersécurité du gouvernement du Canada](#) ou communiquer directement avec la Division de la cybersécurité pour toute question relative à la cybersécurité par courriel à ZZTBSCYBERS@tbs-sct.gc.ca.

- Division Politique sur les services et le numérique
 - Pour toute question relative à la Politique de service et au numérique et aux instruments connexes, veuillez contacter la Division de la Politique sur les services et le numérique, à l'adresse ServiceDigital-ServicesNumerique@tbs-sct.gc.ca.
 - Vous trouverez des informations supplémentaires sur la page [Service et numérique – page GCpédia](#).

- Division de la Politique sur l'accès à l'information et du rendement (DPAIR)
 - Pour obtenir de plus amples informations, veuillez consulter le [site](#) GCpédia de la communauté de l'accès à l'information et de protection des renseignements personnels (AIPRP) ou contactez la Division de la Politique et du rendement de l'accès à l'information pour toute question relative à la gestion et à la prestation des programmes d'accès à l'information, y compris la conformité aux lois et aux politiques de la *Loi sur l'accès à l'information*, à l'adresse ippd-dpiprp@tbs-sct.gc.ca.

- Bureau du dirigeant principal des ressources humaines (BDPRH)
 - Pour en apprendre davantage plus, veuillez consulter le [site](#) Renseignements à l'intention des employés du gouvernement du Canada ou communiquer directement avec le Bureau du dirigeant principal des ressources humaines, aux adresses suivantes :
 - ohs-sst@tbs-sct.gc.ca pour des demandes concernant la santé et la sécurité au travail, y compris le harcèlement et la violence en milieu de travail, et les instruments connexes du SCT.
 - questions@tbs-sct.gc.ca pour toute question relative aux ressources humaines.

- Division de la politique en matière de sécurité
 - Pour de plus amples renseignements, veuillez consulter le [site](#) GCpedia de la PSG du gouvernement ou communiquer avec la Division de la politique en matière de sécurité par courriel à SEC@tbs-sct.gc.ca.

- Division de la protection de la vie privée et des données (DPVPD)
 - Pour obtenir de plus amples renseignements, veuillez consulter le [site](#) GCpédia de la collectivité de l'accès à l'information et de la protection des renseignements personnels (AIPRP) ou communiquer avec la Division de la protection de la vie privée et des données pour toute question relative à la gestion et à la prestation de programmes liés à la protection des renseignements personnels, y compris la conformité aux lois et aux politiques de la *Loi sur la protection des renseignements personnels*, à ippd-dpiprp@tbs-sct.gc.ca