



Directive sur le filtrage de sécurité

Publié : le 2025-01-06

© Sa Majesté le Roi du chef du Canada,
représentée par le président du Conseil du Trésor 2025,

Publié par le Secrétariat du Conseil du Trésor du Canada
90 rue Elgin, Ottawa, Ontario, K1A 0R5, Canada

No de catalogue BT39-85/2025F-PDF
ISBN: 978-0-660-75243-3

Ce document est disponible sur Canada.ca, le site Web du gouvernement du Canada.

Ce document est disponible en médias substituts sur demande.

Nota : Pour ne pas alourdir le texte français, le masculin est utilisé
pour désigner tant les hommes que les femmes.

Also available in English under the title: Directive on Security Screening

Directive sur le filtrage de sécurité

1. Date d'entrée en vigueur

- 1.1 Cette directive entrera en vigueur le 6 janvier 2025.
- 1.2 La présente directive remplace la Norme sur le filtrage de sécurité qui date du 20 octobre 2014.
- 1.3 Élément transitoire à prendre en considération : Dans le cadre de la Norme sur le modèle de filtrage de sécurité et l'analyse des postes, les personnes qui occupent un poste au niveau Très secret ou Très secret approfondi doivent être citoyennes canadiennes. Toutes les personnes occupant ce type de poste seront considérées comme respectant cette exigence au moment où la présente directive entrera en vigueur. Elles continueront de respecter cette exigence tant qu'elles conserveront une autorisation de sécurité valide à ce niveau, jusqu'à un maximum de cinq ans à compter de la date d'entrée en vigueur de cette directive. Cet élément transitoire à prendre en considération ne s'applique pas aux personnes qui demandent une nouvelle autorisation ou dont l'autorisation actuelle est changée pour une autorisation plus élevée ou moins élevée, aux niveaux Très secret et Très secret approfondi.

2. Pouvoirs

- 2.1 La présente directive est émise au titre des pouvoirs figurant à la section 2 de la Politique sur la sécurité du gouvernement.
- 2.2 Le Conseil du Trésor du Canada a délégué au Président du Conseil du Trésor du Canada le pouvoir de modifier ou d'annuler la présente

directive et les instruments à l'appui, notamment les normes, les procédures obligatoires et les autres annexes.

- 2.3 Le Conseil du Trésor du Canada a délégué au président du Conseil du trésor, le pouvoir d'émettre les instruments à l'appui, y compris les normes, les procédures obligatoires et les autres annexes.
- 2.4 Le Conseil du Trésor du Canada a délégué au président du Conseil du trésor le pouvoir d'accorder des dérogations temporaires, au cas par cas, à la présente directive et aux instruments qui l'accompagnent, y compris les normes, les procédures obligatoires et les autres annexes.

3. Objectifs et résultats escomptés

- 3.1 Les objectifs indiqués à la section 3 de la Politique sur la sécurité du gouvernement s'appliquent à cette directive.
- 3.2 Outre les résultats escomptés indiqués à la section 3 de la Politique sur la sécurité du gouvernement, le résultat visé par cette directive est de veiller à ce que les activités de filtrage de sécurité respectent les principes d'équité en matière d'emploi, de diversité et d'inclusion et à ce que ces principes soient appliqués de manière cohérente.

4. Exigences

Dirigeant principal de la sécurité

- 4.1 Le dirigeant principal de la sécurité doit :

Fonction de filtrage de sécurité

- 4.1.1 Diriger et superviser la fonction de filtrage de sécurité du ministère pour :
 - 4.1.1.1 permettre la réalisation cohérente et complète de filtrage de sécurité qui :
 - 4.1.1.1.1 évalue les exigences en matière de filtrage de sécurité pour les postes, les contrats ou d'autres arrangements;

- 4.1.1.1.2 évalue l'admissibilité d'une personne à détenir une cote de sécurité ou d'accès à un site, avant l'obtention d'une autorisation de sécurité ou d'accès à un site;
 - 4.1.1.1.3 informe le processus décisionnel d'octroi, de refus ou de révocation d'une cote ou d'une autorisation de sécurité, ou d'une cote ou d'une autorisation d'accès à un site;
 - 4.1.1.1.4 accorde des droits de révision et de recours qui s'appliquent à toutes les personnes, lorsqu'on décide de refuser, de révoquer ou de suspendre une cote ou une autorisation de sécurité, ou une cote ou une autorisation d'accès à un site;
- 4.1.1.2 veiller à ce que les personnes :
 - 4.1.1.2.1 soient suffisamment fiables pour protéger les renseignements et les biens du gouvernement, y compris les installations et les systèmes de technologie de l'information (TI);
 - 4.1.1.2.2 soient conscients de leurs responsabilités en matière de sécurité;
- 4.1.1.3 veiller à ce que l'effectif ministériel dispose des connaissances, des capacités et des compétences nécessaires pour répondre aux exigences de la fonction de filtrage de sécurité, notamment en respectant les valeurs et les principes du gouvernement du Canada;

- 4.1.1.4 conserver un dossier de sécurité pour toutes les personnes faisant l'objet d'un filtrage de sécurité, conformément à la Loi sur la protection des renseignements personnels et aux instruments de politique connexes du gouvernement du Canada;
- 4.1.1.5 veiller à ce que les renseignements personnels destinés au filtrage de sécurité soient :
 - 4.1.1.5.1 recueillis, créés, utilisés, divulgués, conservés et éliminés conformément à la Loi sur la protection des renseignements personnels et aux instruments de politique du gouvernement du Canada;
- 4.1.1.6 élaborer et mettre en œuvre des processus d'échange de renseignements au sein du ministère et avec d'autres ministères qui :
 - 4.1.1.6.1 sont définis et mis en œuvre;
 - 4.1.1.6.2 cadrent avec les orientations du gouvernement canadien en matière de gestion des renseignements relatifs au filtrage de sécurité;
 - 4.1.1.6.3 sont conformes à la Loi sur la protection des renseignements personnels et aux instruments de politique du gouvernement du Canada en matière de traitement des renseignements personnels;
 - 4.1.1.6.4 facilitent l'acceptation des dossiers de filtrage de sécurité d'autres ministères et leur transfert;
 - 4.1.1.6.5 permettent l'échange de renseignements au sein du ministère et

avec d'autres ministères, lorsqu'on décide de refuser, de révoquer ou de suspendre une cote ou une autorisation de sécurité, ou une cote ou une autorisation d'accès à un site.

- 4.1.2 Lorsque des personnes externes au gouvernement doivent faire l'objet d'un filtrage de sécurité et que le ministère doit donc leur transmettre des renseignements ou des biens sensibles, ou leur donner accès des installations ou à des systèmes de TI sensibles, il convient de veiller à ce que :
- 4.1.2.1 les exigences en matière de filtrage de sécurité pour les entrepreneurs et autres personnes soient détaillées dans les documents pertinents (voir l'annexe F – Procédures obligatoires relatives aux mesures de sécurité lors de l'octroi de contrats et d'autres ententes de la Directive sur la gestion de la sécurité);
 - 4.1.2.2 la cote ou l'autorisation de sécurité requise soit accordée avant que l'information ne soit partagée et que l'accès ne soit fourni.

Services interministériels de filtrage de sécurité

- 4.1.3 Utiliser les services de filtrage de sécurité lorsqu'ils sont obligatoires ou disponibles pour répondre aux exigences ministérielles en matière de filtrage de sécurité et :
- 4.1.3.1 veiller à ce que les services obtenus répondent à ces exigences.
- 4.1.4 Veiller à la mise en place d'un accord écrit lorsque l'organisation fournit ou reçoit des services de filtrage de sécurité d'une autre organisation conformément aux paragraphes 6.3 et 6.4, qui :
- 4.1.4.1 définissent les exigences applicables en matière de sécurité et de respect de la vie privée, en

collaboration avec les fonctionnaires ministériels concernés;

4.1.4.2 établissent les responsabilités respectives en matière de filtrage de sécurité.

4.1.5 Lorsque la fonction de filtrage de sécurité implique la prestation de services aux ministères clients :

4.1.5.1 confirmer que les exigences en matière de filtrage de sécurité pour les postes des ministères clients sont élaborées sous la direction du dirigeant principal de la sécurité du ministère client;

4.1.5.2 avant de recommander une décision d'octroi, d'octroi sous conditions, de refus ou de révocation d'une cote ou d'une autorisation de sécurité, consulter le dirigeant principal de la sécurité et, le cas échéant, l'administrateur général du ministère client.

Risque de sécurité et renseignements défavorables

4.1.6 Prendre des mesures pour faire face à tout risque de sécurité présentant des menaces graves et immédiates pour la sécurité des personnes, des renseignements ou des biens du ministère, ou du gouvernement du Canada et, le cas échéant :

4.1.6.1 consulter la direction des ressources humaines au sujet de la suspension de la cote ou de l'autorisation de sécurité d'un employé;

4.1.6.2 consulter l'autorité contractante au sujet de la suspension du contrat d'un entrepreneur :

4.1.6.2.1 cote ou autorisation de sécurité;

4.1.6.2.2 cote ou autorisation d'accès aux sites;

- 4.1.6.3 suspendre la cote ou l'autorisation de sécurité ou la cote ou l'autorisation d'accès au site de la personne, en attendant l'issue d'une enquête;
- 4.1.6.4 suspendre la cote ou l'autorisation de sécurité ou la cote ou l'autorisation d'accès au site de la personne lorsqu'elle refuse de fournir son consentement ou le retire après 30 jours de suspension;
- 4.1.6.5 signaler ces événements relatifs à la sécurité à l'organisme chargé de l'application de la loi ou au service de renseignement et de sécurité compétent (voir l'annexe I – Norme sur le signalement des incidents de sécurité de la Directive sur la gestion de la sécurité).

Demandes de modification

- 4.1.7 Aider l'administrateur général à obtenir l'approbation du président du Conseil du Trésor pour toute exception temporaire à l'application de la présente directive et des instruments connexes, notamment les normes, les procédures obligatoires et les autres annexes, en consultation avec le Secrétariat du Conseil du Trésor du Canada et d'autres parties prenantes.

Gestion du cycle de vie

- 4.1.8 Établir et superviser la mise en œuvre et l'examen des pratiques en matière de filtrage de sécurité pour les postes et les personnes :
 - 4.1.8.1 définir, consigner et mettre en œuvre des pratiques ministérielles pour le cycle de vie de l'analyse des postes et du filtrage de sécurité;
 - 4.1.8.2 assurer l'harmonisation avec les pratiques de gestion de la direction des ressources humaines du ministère.

Suivi et établissement de rapports

- 4.1.9 Surveiller la conformité à la présente directive :
 - 4.1.9.1 évaluer, examiner et signaler à l'administrateur général tout problème de conformité important;
 - 4.1.9.2 prendre les mesures demandées par l'administrateur général.
- 4.1.10 Consigner et contrôler les pratiques en matière de filtrage de sécurité afin de répondre aux exigences de sécurité indiquées pour les programmes, les services et les activités et :
 - 4.1.10.1 assurer le respect continu des pratiques en matière de filtrage de sécurité.
- 4.1.11 Collaborer avec les hauts fonctionnaires et d'autres intervenants pour répondre aux demandes d'orientation, de conseils et d'information émises par le Secrétariat du Conseil du Trésor du Canada.
- 4.1.12 Fournir des renseignements au Secrétariat du Conseil du Trésor du Canada sur demande.

Hauts fonctionnaires de la gouvernance de la sécurité ministérielle

- 4.2 Les hauts fonctionnaires, désignés par l'administrateur général pour la gouvernance de la sécurité du ministère, doivent :

Fonction de filtrage de sécurité

- 4.2.1 Participer et se rapporter à la gouvernance ministérielle de sécurité.
- 4.2.2 Collaborer avec les hauts fonctionnaires, les spécialistes fonctionnels de la sécurité, les partenaires et d'autres intervenants pour :
 - 4.2.2.1 déterminer les exigences en matière de filtrage de sécurité et les besoins en ressources connexes

- pour les programmes, les services et les activités;
- 4.2.2.2 documenter et mettre en œuvre des pratiques en matière de filtrage de sécurité pour répondre aux exigences de sécurité indiquées pour les programmes, les services et les activités;
- 4.2.2.3 assurer le respect continu des pratiques en matière de filtrage de sécurité;
- 4.2.2.4 attribuer des responsabilités en matière de filtrage de sécurité pour les programmes, les services et les activités;
- 4.2.2.5 documenter et mettre en œuvre les pratiques en ce qui concernent les droits de recours et de révision pour les activités de filtrage de sécurité;
- 4.2.2.6 fournir des conseils à l'administrateur général, au dirigeant principal de la sécurité et à d'autres intervenants sur les questions relatives au filtrage de sécurité ministériel dans leur domaine de responsabilité.

Services interministériels de filtrage de sécurité

- 4.2.3 Lorsque la fonction de filtrage de sécurité consiste à fournir des services à un autre ministère ou à s'en remettre à lui, veiller à ce que :
 - 4.2.3.1 Un soutien est apporté au dirigeant principal de la sécurité pour respecter le paragraphe 4.1.4 de la présente directive afin :
 - 4.2.3.1.1 de respecter les exigences et les responsabilités de l'entente;
 - 4.2.3.1.2 d'assurer le suivi de la conformité.

Risques liés à la sécurité et renseignements défavorables

- 4.2.4 Traiter les renseignements défavorables, en collaboration avec le dirigeant principal de la sécurité, les partenaires et d'autres intervenants;

Suivi et établissement de rapports

- 4.2.5 Assurer le suivi de l'efficacité des pratiques en matière de filtrage de sécurité dans leur secteur de responsabilité et en rendre compte, et communiquer les résultats au dirigeant principal de la sécurité.

Spécialistes fonctionnels de la sécurité et autres personnes désignées

- 4.3 Les spécialistes fonctionnels de la sécurité et les autres personnes désignées dans le cadre de la gouvernance de la sécurité ministérielle doivent :

- 4.3.1 Assurer la coordination et le soutien nécessaires pour ce qui est du filtrage de sécurité du ministère afin de :

- 4.3.1.1 mettre en œuvre les pratiques ministérielles en matière de filtrage de sécurité telles qu'elles sont prescrites dans les annexes de la présente directive.

- 4.3.2 Assurer le suivi et rendre compte de l'efficacité des pratiques en matière de filtrage de sécurité, et communiquer les résultats au dirigeant principal de la sécurité afin :

- 4.3.2.1 d'évaluer la mesure dans laquelle les exigences de sécurité du ministère sont respectées;

- 4.3.2.2 de déterminer les mesures nécessaires en cas d'insuffisance.

- 4.3.3 Fournir des conseils au dirigeant principal de la sécurité et aux autres intervenants, le cas échéant, sur les questions de filtrage de sécurité au sein du ministère.

Gestionnaires

4.4 Les personnes ayant des responsabilités en ressources humaines doivent :

4.4.1 Intégrer les facteurs à prendre en compte relativement au filtrage de sécurité dans la planification et les autres activités administratives;

4.4.2 Collaborer avec le dirigeant principal de la sécurité pour déterminer le niveau de filtrage approprié pour chaque poste sous leur responsabilité :

4.4.2.1 conformément aux paragraphes A.2.2.4 et A.2.2.10 de l'annexe A – Norme sur le modèle de filtrage de sécurité et l'analyse des postes.

4.4.3 Veiller à ce que l'exigence établie d'une cote ou d'une autorisation de sécurité comme condition préalable à un emploi, une nomination, un contrat ou un autre arrangement, ou d'une affectation à des postes sous leur responsabilité, soit reflétée dans les documents pertinents;

4.4.4 Veiller à ce que les personnes sous leur responsabilité actuelle ou future aient une cote ou une autorisation de sécurité valide, telle que définie par les exigences du ministère en matière de filtrage de sécurité, avant :

4.4.4.1 de faire une offre d'emploi inconditionnelle;

4.4.4.2 d'attribuer un contrat;

4.4.4.2.1 de permettre à un entrepreneur, au cours de la phase précontractuelle, d'accéder à des renseignements sensibles dans le cadre d'un appel d'offres;

4.4.4.3 de les placer dans un poste au moyen d'un autre mécanisme, comme une affectation, un

détachement, un bénévolat ou une autre capacité officielle;

4.4.4.4 de permettre l'accès à des biens et à des renseignements sensibles, notamment des installations et des systèmes de TI.

4.4.5 Veiller à ce que les personnes sous leur responsabilité aient assisté à une séance d'information en matière de sécurité avant d'obtenir l'accès aux renseignements sensibles et aux biens, y compris les installations et les systèmes de TI;

4.4.6 Signaler au dirigeant principal de la sécurité les changements dans la situation personnelle et le comportement des personnes sous leur responsabilité qui pourraient avoir une incidence sur la cote ou l'autorisation de sécurité qui leur a été accordée.

Personnes

4.5 Les personnes doivent :

4.5.1 Fournir leur consentement pour lancer les activités de filtrage.

4.5.2 Fournir les renseignements personnels et les documents de preuve requis pour le filtrage de sécurité qui sont :

4.5.2.1 exacts et vrais;

4.5.2.2 conformes au format requis et aux délais et cycles de mise à jour établis.

4.5.3 Indiquer qu'elles comprennent et acceptent les responsabilités en matière de sécurité en signant le Certificat d'enquête de sécurité et profil de sécurité.

4.5.4 Accomplir leurs tâches de manière fiable en respectant :

4.5.4.1 la cote ou l'autorisation de sécurité qui leur est accordée;

- 4.5.4.2 les obligations en matière de sécurité décrites en détail dans le Certificat de filtrage de sécurité et profil de sécurité;
- 4.5.4.3 les politiques de sécurité du gouvernement et les pratiques ministérielles en matière de sécurité, notamment la protection de l'information et des biens placés sous leur contrôle, qu'elles travaillent sur place ou à l'extérieur.
- 4.5.5 Aviser leur gestionnaire ou le dirigeant principal de la sécurité de ce qui suit :
 - 4.5.5.1 les renseignements liés à un changement de situation personnelle;
 - 4.5.5.2 tout contact persistant ou inhabituel, ou toute tentative par une personne, un groupe, une organisation ou une autre entité de solliciter ou d'obtenir l'accès à des biens et à des renseignements sensibles, notamment des installations et des systèmes de TI, sans autorisation; ou
 - 4.5.5.3 le comportement de personnes susceptibles de présenter un risque pour la sécurité du ministère ou du gouvernement du Canada (tel que décrit à l'annexe G – Procédures obligatoires relatives à l'octroi, au maintien et à l'assurance du filtrage de sécurité d'une personne).

Personnes désignées par les administrateurs généraux des organisations de services internes intégrés pour superviser leurs activités de services internes intégrés

- 4.6 Les personnes désignées par les administrateurs généraux des organisations de services internes intégrés autorisées à fournir des services de filtrage de sécurité aux ministères doivent :

Fonction de filtrage de sécurité

- 4.6.1 Soutenir l'administrateur général, le dirigeant principal de la sécurité et d'autres parties prenantes, le cas échéant, sur les questions de filtrage de sécurité du ministère, notamment :
- 4.6.1.1 veiller à la mise en place d'un accord écrit pour les services de filtrage de sécurité fournis à d'autres organisations conformément aux paragraphes 6.3 et 6.4.
- 4.6.2 Mettre à la disposition de l'administrateur général ou du dirigeant principal de la sécurité d'un ministère client les éléments suivants sur demande et en temps opportun :
- 4.6.2.1 les renseignements relatifs aux activités et aux résultats du filtrage de sécurité, à moins que la loi ne l'interdise, notamment la Loi sur la protection des renseignements personnels et la Loi sur le casier judiciaire ou toute autre loi applicable;
- 4.6.2.2 les conseils et recommandations visant à étayer les résultats des activités de filtrage de sécurité et à éclairer la prise de décision.
- 4.6.3 Maintenir un dossier de sécurité pour toutes les personnes faisant l'objet d'un filtrage de sécurité conformément à Loi sur la protection des renseignements personnels et aux instruments de politique connexes du gouvernement du Canada.
- 4.6.4 Veiller à ce que les renseignements personnels destinés au filtrage de sécurité soient :
- 4.6.4.1 recueillis, créés, utilisés, divulgués, conservés et éliminés conformément à la Loi sur la protection des renseignements personnels et aux instruments de politique du gouvernement du Canada.

Filtrage de sécurité des services internes intégrés

- 4.6.5 Veiller à ce que les personnes ou les organisations auxquelles on confie la responsabilité d'effectuer le filtrage de sécurité soient qualifiées pour le faire. Elles doivent notamment :
- 4.6.5.1 s'acquitter de leurs responsabilités conformément aux exigences légales et politiques en tenant compte des intérêts du Canada en matière de sécurité;
 - 4.6.5.2 assurer le suivi de la conformité des services de filtrage de sécurité par rapport aux normes de service établies;
 - 4.6.5.3 signaler aux ministères concernés et au Secrétariat du Conseil du Trésor du Canada tout problème lié à la prestation de services de filtrage de sécurité.

Surveillance et établissement de rapports

- 4.6.6 Assurer la surveillance de la conformité à la présente directive :
- 4.6.6.1 évaluer, examiner et signaler à l'administrateur général tout problème de conformité important;
 - 4.6.6.2 mettre en œuvre les mesures demandées par l'administrateur général;
 - 4.6.6.3 rendre compte des résultats au Secrétariat du Conseil du Trésor du Canada, notamment les renseignements contribuant à la supervision et à l'orientation stratégique dans l'ensemble du gouvernement.
- 4.6.7 Collaborer avec les hauts fonctionnaires et d'autres intervenants pour répondre aux demandes d'orientation, de conseils et d'information émises par le Secrétariat du Conseil du Trésor du Canada.

5. Rôles des autres organisations gouvernementales

- 5.1 Cet article indique les principales organisations gouvernementales concernées par la Politique sur la sécurité du gouvernement. En soi, cet article ne confère aucune autorisation.
- 5.2 Cette section indique les principaux organismes de sécurité ou les organisations de services internes intégrés qui fournissent la direction et l'appui dans le cadre de la présente directive et qui contribuent à la réalisation des objectifs de la Politique sur la sécurité du gouvernement. Elle indique les responsabilités de chacune des organisations, conformément à leurs mandats respectifs.
- 5.3 Les responsabilités et les rôles suivants s'ajoutent à ceux qui sont énoncés dans la Politique sur la sécurité du gouvernement.
- 5.4 Le Service canadien du renseignement de sécurité est responsable de ce qui suit :
 - 5.4.1 Procéder, pour le compte des ministères, à l'évaluation de la loyauté des une personnes envers le Canada et, dans la mesure où elle s'y rapporte, leur fiabilité.
- 5.5 Le Centre de la sécurité des télécommunications est responsable de ce qui suit :
 - 5.5.1 Définir des critères et des systèmes de contrôle formels pour l'accès à l'information cloisonnée du renseignement d'origine électromagnétique (SIGINT) pour autoriser les services gouvernementaux à effectuer des endoctrinements et à tenir le registre national du personnel endoctriné.
- 5.6 Défense nationale est responsable de ce qui suit :
 - 5.6.1 Traiter les demandes de visites lorsque le personnel militaire ayant obtenu une cote de sécurité doit se rendre dans un établissement gouvernemental ou militaire au Canada ou à l'étranger.

- 5.6.2 Établir les critères et les systèmes de contrôle officiels d'accès à des informations cloisonnées de Talent-Keyhole (TK) afin d'autoriser les ministères gouvernementaux à effectuer des endoctrinements et de tenir à jour le registre national du personnel endoctriné.
- 5.7 Affaires mondiales Canada est responsable de ce qui suit :
 - 5.7.1 Effectuer le filtrage de sécurité du personnel recruté localement et des fonctionnaires d'autres gouvernements dans les missions canadiennes à l'étranger.
- 5.8 Services publics et Approvisionnement Canada est responsable de ce qui suit :
 - 5.8.1 Effectuer le filtrage de sécurité des entrepreneurs, d'autres personnes et d'entités organisationnelles dans le cadre du processus d'octroi de contrats du gouvernement, y compris de ceux qui participent à des marchés étrangers.
 - 5.8.2 Gérer un système de demande de permis de visite pour les visiteurs ayant accès à des renseignements classifiés dans des locaux du secteur privé et pour des particuliers du secteur privé de l'étranger qui ont accès à des renseignements classifiés dans des locaux du gouvernement.
- 5.9 La Gendarmerie royale du Canada est responsable de ce qui suit :
 - 5.9.1 Effectuer les vérifications du casier judiciaire et les vérifications des dossiers policier, en vue de vérifier si une personne a été trouvée coupable d'un acte criminel et, au besoin, évaluer sa participation à des organisations criminelles ou à des activités criminelles.
- 5.10 Le Secrétariat du Conseil du Trésor du Canada est responsable de ce qui suit :
 - 5.10.1 Déterminer les renseignements personnels à recueillir, à utiliser, à communiquer, à conserver et à éliminer aux fins du filtrage de sécurité, et maintenir la description figurant au

6. Application

- 6.1 La présente directive s'applique aux organisations indiquées dans le paragraphe 6.1 de la Politique sur la sécurité du gouvernement.
- 6.2 Les administrateurs généraux des organisations suivantes sont les seuls responsables d'assurer le contrôle et le respect de la présente directive au sein de leur organisation :
- Bureau du vérificateur général du Canada
 - Bureau du directeur général des élections
 - Commissariat au lobbying du Canada
 - Commissariat aux langues officielles
 - Commissariat à l'information du Canada
 - Commissariat à la protection de la vie privée du Canada
 - Commissariat à l'intégrité du secteur public du Canada
- 6.3 Les paragraphes 4.1.4 et 4.2.3.1 de la présente directive ne s'appliquent qu'aux accords interministériels conclus en vertu du paragraphe 29.2 de la Loi sur la gestion des finances publiques et aux ententes conclues avec des sociétés d'État, d'autres organes du gouvernement, le secteur privé ou d'autres entités qui ne sont pas régies par la Politique sur la sécurité du gouvernement, lorsque le ministère a le pouvoir de conclure de tels accords ou de telles ententes.
- 6.4 Les paragraphes 4.1.4 et 4.2.3.1 de la présente directive s'appliquent aux contrats de production ou de livraison de biens ou de services, et à toute autre entente exigeant l'échange de biens ou de renseignements sensibles avec des organisations ou des personnes qui ne sont pas assujetties à la Politique sur la sécurité du gouvernement.

7. Références

- 7.1 Législation

- Loi sur l'accès à l'information
- Charte canadienne des droits et libertés
- Loi canadienne sur les droits de la personne
- Loi sur le Service canadien du renseignement de sécurité
- Code criminel
- Loi sur le casier judiciaire
- Loi sur l'équité en matière d'emploi
- Loi sur la Commission des relations de travail et de l'emploi dans le secteur public fédéral
- Loi sur les relations de travail dans le secteur public fédéral
- Loi sur la gestion des finances publiques
- Loi sur les enquêtes
- Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement
- Loi sur les langues officielles
- Loi sur la protection des renseignements personnels;
- Loi sur l'emploi dans la fonction publique
- Loi sur la communication d'information ayant trait à la sécurité du Canada
- Loi sur l'ingérence étrangère et la protection de l'information
- Loi sur le système de justice pénale pour les adolescents

7.2 Instruments de politique connexes

- Cadre principal des politiques du Conseil du trésor
- Politique sur la sécurité du gouvernement
- Politique sur la gestion des personnes
- Politique sur les services et le numérique
- Politique sur la protection de la vie privée
- Politiques à l'intention des cabinets des ministres
- Code de valeurs et d'éthique du secteur public
- Directive sur la gestion de l'approvisionnement
- Directive sur la gestion de l'identité
- Directive sur les services et le numérique
- Directive sur les pratiques relatives à la protection de la vie privée
- Directive sur l'évaluation des facteurs relatifs à la vie privée

- Directive sur les demandes de renseignements personnels et de correction des renseignements personnels
- Directive sur la gestion de la sécurité
- Directive sur la prise de décisions automatisée
- Directive sur l'équité en matière d'emploi, la diversité et l'inclusion

7.3 Orientations connexes

- Ligne directrice sur l'assurance de l'identité
- Ligne directrice sur les services et le numérique
- Lignes directrices concernant la discipline
- Lignes directrices concernant le licenciement ou la rétrogradation pour rendement insatisfaisant; le licenciement ou la rétrogradation pour des raisons autres qu'un manquement à la discipline ou une inconduite; et le licenciement en cours de stage
- Document d'orientation : Prise en compte de la protection des renseignements personnels avant de conclure un marché
- Avis de mise en œuvre sur la protection des renseignements personnels 2023-03 : Orientation relative à la collecte, à l'utilisation, à la conservation et à la divulgation de renseignements personnels accessibles au public en ligne

8. Demandes d'information

- 8.1 Les membres du grand public peuvent communiquer avec le personnel chargé des demandes de renseignements du Secrétariat du Conseil du Trésor du Canada pour obtenir de plus amples renseignements sur la présente directive.
- 8.2 Les employés des ministères doivent communiquer avec leur groupe de gestion de la sécurité ministérielle s'ils ont des questions au sujet de la présente directive.
- 8.3 Les membres du groupe de sécurité ministériel peuvent communiquer avec la Division de la politique de sécurité du Secrétariat du Conseil du Trésor du Canada par courriel à l'adresse

Annexe A. Norme sur le modèle de filtrage de sécurité et l'analyse des postes

A.1 Date d'entrée en vigueur

A.1 La présente norme entre en vigueur le 6 janvier 2025.

A.2 Normes

A.2.1 La présente norme fournit des renseignements sur les exigences énoncées aux paragraphes 4.1.1.1 et 4.6.1 de la Directive sur le filtrage de sécurité.

A.2.2 Les normes sont les suivantes :

A.2.2.1 accorder une cote ou une autorisation au niveau requis en fonction de ce qui suit :

A.2.2.1.1 le poste que la personne occupe; ou

A.2.2.1.2 le contrat ou autre entente auquel la personne participe.

Modèle de filtrage de sécurité pour les personnes

A.2.2.2 Procéder à un filtrage de sécurité :

A.2.2.2.1 pour tous les postes ou toutes les fonctions au sein du gouvernement du Canada;

A.2.2.2.2 pour tous les contrats ou autres ententes nécessitant l'échange de bien et de renseignements sensibles ou l'accès à de tels biens et renseignements, notamment les installations et les systèmes de TI;

A.2.2.2.3 conformément à l'annexe A1.

A.2.2.3 Évaluer :

- A.2.2.3.1 la fiabilité, l'honnêteté et la confiance en tant que critère d'admissibilité à détenir une cote;
- A.2.2.3.2 la fiabilité, l'honnêteté, la confiance, la loyauté envers le Canada et la fiabilité en ce qui a trait à cette loyauté en tant que critère d'admissibilité à recevoir une autorisation.

Analyse des postes des personnes

A.2.2.4 Déterminer le niveau de sécurité requis pour les postes en fonction de ce qui suit :

- A.2.2.4.1 tâches à accomplir;
- A.2.2.4.2 niveau d'autorité ou de contrôle exercé par le titulaire du poste;
- A.2.2.4.3 sensibilité des renseignements et des biens, y compris les installations et les systèmes de TI auxquels il faut accéder, notamment :
 - A.2.2.4.3.1 le degré de préjudice qui pourrait découler de la compromission,
 - A.2.2.4.3.2 le principe du besoin de connaître ou du besoin d'accéder;
- A.2.2.4.4 au minimum, tous les postes sont établis à la cote de fiabilité lorsqu'ils sont occupés par des employés ou d'autres personnes travaillant dans les ministères, comme défini à l'article 2, et dans tout autre organisme figurant aux annexes IV et V de la *Loi sur la gestion des finances publiques*, sauf s'ils en sont exclus au titre d'une loi, d'un règlement ou d'un décret particulier;
- A.2.2.4.5 conformément aux critères définis à l'annexe A2.

A.2.2.5 N'accorder des autorisations Très secret ou Très secret approfondie qu'à des employés ou autres personnes ayant la citoyenneté canadienne.

A.2.2.6 Étendre le filtrage de sécurité au niveau approfondie conformément aux critères énoncés à l'annexe A2.

Exigences en matière de sécurité pour les contrats et d'autres ententes

A.2.2.7 Conformément à l'annexe F – Procédures obligatoires relatives aux mesures de sécurité lors de l'octroi de contrats et d'autres ententes de la Directive sur la gestion de la sécurité, les contrats et autres ententes dont les exigences de sécurité nécessitent une autorisation Très secret ou Très secret approfondie ne peuvent être accordés qu'à des entrepreneurs ou à d'autres personnes ayant la citoyenneté canadienne.

Modèle de contrôle d'accès au site pour les non-employés

A.2.2.8 Appliquer un contrôle d'accès au site :

A.2.2.8.1 pour les individus qui ne sont pas des employés et qui ont besoin d'accéder à des zones ou à des installations protégées ou à accès restreint;

A.2.2.8.2 conformément à l'annexe A3.

A.2.2.9 Évaluer :

A.2.2.9.1 la fiabilité, l'honnêteté et la confiance en tant que critère d'admissibilité à détenir une cote;

A.2.2.9.2 la fiabilité, l'honnêteté, la confiance, la loyauté envers le Canada et la fiabilité en ce qui a trait à cette loyauté en tant que critère d'admissibilité à recevoir une autorisation.

Analyse des postes des non-employés

A.2.2.10 Déterminer le niveau de contrôle d'accès au site requis pour les contrats ou autres ententes en fonction de ce qui suit :

A.2.2.10.1 la sensibilité et la nature des programmes, services et activités du ministère;

A.2.2.10.2 la nature des tâches ou des services à accomplir;

A.2.2.10.3 si la personne est escortée ou non;

A.2.2.10.4 si la personne doit avoir accès à l'extérieur ou à l'intérieur d'une installation;

A.2.2.10.5 le risque que la personne voie ou entende par inadvertance des renseignements ou des conversations sensibles;

A.2.2.10.6 la conformité aux critères définis à l'annexe A4.

Annexe A1. Niveaux de filtrage de sécurité et activités connexes

Niveau	Activités de filtrage de sécurité	Niveau	Activités de filtrage de sécurité
Cote de fiabilité Validité : 10 ans	• Vérification de l'identité. • Vérification de 5 ans d'antécédents • Vérification des diplômes et des désignations professionnelles • Vérification des références personnelles et professionnelles. • Enquête sur la situation financière (vérification de solvabilité) • Vérification du casier judiciaire	Cote de fiabilité approfondie Validité : 10 ans	Ensemble des activités pour la cote de fiabilité ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité

Niveau	Activités de filtrage de sécurité	Niveau	Activités de filtrage de sécurité
Autorisation de niveau Secret Validité : 10 ans	Ensemble des activités pour la cote de fiabilité ainsi que : • Vérification de 10 ans d'antécédents • Évaluation de sécurité du SCRS	Autorisation de niveau Secret approfondie Validité : 10 ans	Ensemble des activités pour l'autorisation de niveau Secret ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité
Autorisation de niveau Très secret Validité : 5 ans	Ensemble des activités pour l'autorisation de niveau Secret ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité • Voyages à l'étranger, passeports, actifs et service militaire • Citoyenneté canadienne	Autorisation de niveau Très secret approfondie Validité : 5 ans	Ensemble des activités pour l'autorisation de de niveau Très secret ainsi que : • Test polygraphique

Annexe A2. Critères applicables pour déterminer le niveau du

filtrage de sécurité

Niveau	Critères applicables pour déterminer le niveau	Permissions d'accès
Cote de fiabilité	- Effectuer le filtrage des personnes pour la cote de fiabilité : - lorsque les postes exigent : - un accès sans supervision à des renseignements et biens du gouvernement du Canada; - un accès sans escorte aux zones de sécurité physique dans les installations où des renseignements protégés du gouvernement du Canada sont traités; ou - accès au niveau de l'utilisateur aux systèmes de TI de catégorie Protégé A ou Protégé B. - en tant que contrôle minimal pour tous les postes.	Accès à des renseignements des biens des systèmes de catégorie Protégé A Protégé B
Autorisation de niveau Secret	- Effectuer le filtrage des personnes pour l'autorisation de niveau Secret : - s'appuyant sur les critères de filtrage pour une cote de fiabilité, et lorsque les postes exigent : - un accès non surveillé à des renseignements et biens de catégorie Secret du gouvernement du Canada; - un accès sans escorte aux zones de sécurité physique dans les installations du gouvernement où des renseignements de niveau Secret sont traités; ou - un accès au niveau de l'utilisateur aux systèmes de TI de catégorie Secret.	- Accès à des renseignements des biens des systèmes de catégorie Protégé A Protégé B Confidential Secret - Accès aux systèmes de catégorie Protégé A Protégé B Confidential Secret - Privilèges accrus (ou administrateur) aux systèmes de TI

Niveau	Critères applicables pour déterminer le niveau	Permissions d'accès
Autorisation de niveau Secret approfondie	• Effectuer le filtrage des personnes pour l'autorisation de niveau Secret approfondie : ◦ s'appuyant sur les critères de filtrage pour une autorisation de niveau Secret, et lorsque les postes exigent : ▪ que des personnes exercent des fonctions de sécurité et de renseignement, notamment : ▪ l'accès non contrôlé à des renseignements ou à des biens de catégorie Secret liés à l'exécution de la loi ou de nature criminelle, y compris les systèmes de TI et l'accès sans escorte à des zones de sécurité physique dans des installations où ces renseignements sont traités ou stockés; ou ▪ les tâches qui appuient ces fonctions et qui : ▪ exigent un accès sans supervision à des renseignements ou à des biens Secrets liés à l'exécution de la loi.	• Accès aux renseignements aux systèmes de TI et aux biens de catégorie Protégé A, Protégé B, Protégé C, Confidentiel et Secret • Privilèges administratifs accrus (ou administratifs) aux systèmes de TI

Niveau	Critères applicables pour déterminer le niveau	Permissions d'accès
Autorisation de niveau Très secret approfondie	• Effectuer le filtrage des personnes pour l'autorisation de niveau Très secret approfondie: ◦ s'appuyant sur le critère de filtrage pour une autorisation de niveau Très secret, et lorsque les postes exigent : ▪ que des personnes exercent des fonctions de défense, de sécurité et de renseignement, notamment : ▪ l'accès non contrôlé à des renseignements ou à des biens de catégorie Très secret, y compris des systèmes de TI, liés à l'exécution de la loi ou de nature criminelle; ▪ l'accès sans supervision aux méthodes, aux sources, aux processus analytiques, aux plans et aux techniques liés à la collecte d'information sensible en matière de renseignement ou de contre-ingérence; ▪ l'accès sans escorte aux zones de sécurité physique dans les installations où des renseignements liés à l'exécution de la loi ou de nature criminelle sont traités ou stockés; ou ▪ les tâches qui appuient ces fonctions et qui : ▪ exigent un accès sans supervision à des biens Très secret; ou ▪ un accès sans escorte aux zones de sécurité physique au sein des installations où ces renseignements	• Accès à des renseignements à des biens de catégorie Très secret des systèmes de TI du gouvernement protégés classifiés (importe le niveau)

Niveau	Critères applicables pour déterminer le niveau	Permissions d'
	sont traités ou stockés.	

Annexe A3. Niveaux de contrôle d'accès aux sites et activités connexes

Niveau	Activités
Cote d'accès aux sites Validité : 10 ans	• Vérification de l'identité • Vérification de 5 ans d'antécédents • Vérification du casier judiciaire
Autorisation d'accès aux sites Validité : 10 ans	Ensemble des activités relatives à la cote d'accès aux sites ainsi que : • Évaluation de sécurité du SCRS
Desactivités supplémentaires peuvent être effectuées conformément au paragraphe A.2.2.10 – Analyse des postes des non-employés	Ensemble des activités liées à l'autorisation d'accès aux sites ainsi que : • Références personnelles et professionnelles. • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité • Test polygraphique

Annexe A4. Critères applicables pour déterminer le niveau de

contrôle d'accès aux sites

Niveau	Critères applicables pour déterminer le niveau	Permissions d'accès
Cote d'accès aux sites	• Effectuer le filtrage des personnes pour la cote d'accès aux sites : ◦ en tant que niveau de filtrage minimum pour l'accès aux sites dans les cas où il est nécessaire : ▪ d'accéder aux zones où des renseignements et des biens protégés sont traités ou stockés; ou ▪ d'accéder au besoin à des zones d'accès restreint faisant partie d'une <u>hiérarchie contrôlée des zones de sécurité physique</u>. ◦ quand l'accès à des renseignements gouvernementaux sensibles n'est pas requis; ◦ quand l'individu n'est pas un employé.	• Accès sans escorte aux installations du gouvernement fédéral et aux zones d'accès restreint dans ces installations • Pas d'accès à l'information

Niveau	Critères applicables pour déterminer le niveau	Permissions d'accès
Autorisation d'accès aux sites	• Effectuer le filtrage des personnes pour l'autorisation d'accès aux sites : ◦ s'appuyant sur le critère de filtrage pour une cote d'accès aux sites et dans les cas où il est nécessaire : ▪ d'accéder aux zones où des renseignements et des biens classifiés sont traités ou stockés; ▪ d'accéder au besoin à des zones d'accès restreint d'installations des forces de l'ordre; ou ▪ d'accéder au besoin à des zones d'accès restreint faisant partie d'une <u>hiérarchie contrôlée des zones de sécurité physique</u>; ◦ quand l'accès à des renseignements gouvernementaux sensibles n'est pas requis; ◦ quand l'individu n'est pas un employé.	• Accès sans escorte aux installations du gouvernement fédéral et aux zones d'accès restreint dans ces installations • Accès sans escorte aux installations des forces de l'ordre public • Pas d'accès à l'information

Annexe B. Procédures obligatoires pour la gestion des renseignements personnels aux fins de filtrage de sécurité

B.1 Date d'entrée en vigueur

B.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

B.2 Procédures

B.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.1, 4.1.1.4 et 4.1.1.5, 4.1.1.6, 4.6.1, 4.6.3 et 4.6.4 de la Directive sur le filtrage de sécurité.

B.2.2 Voici les procédures obligatoires.

La sécurité des renseignements personnels

B.2.2.1 Attribuer une catégorie de sécurité aux renseignements personnels, en fonction de leur sensibilité et conformément à l'annexe E – Procédures obligatoires relatives aux mesures de sécurité de la gestion de l'information de la Directive sur la gestion de la sécurité.

B.2.2.1.1 Mettre en œuvre des mesures pour protéger les renseignements sensibles au moyen de mesures de sécurité appropriées.

Collecte et création de renseignements personnels : fichiers de renseignements personnels

B.2.2.2 Recueillir, créer, utiliser, divulguer, conserver et éliminer des renseignements personnels à des fins de filtrage de sécurité conformément à la Loi sur la protection des renseignements personnels et à la Directive sur les pratiques relatives à la protection de la vie privée.

Formulaires et modèles de filtrage de sécurité

B.2.2.3 Recueillir des renseignements personnels en utilisant les formulaires et les modèles prescrits par le Secrétariat du Conseil du Trésor du Canada.

Consentement concernant la collecte, l'utilisation et la communication

B.2.2.4 Conformément à la Directive sur les pratiques relatives à la protection de la vie privée, avant la collecte, l'utilisation ou la divulgation de renseignements, obtenir un consentement éclairé de ce qui suit :

B.2.2.4.1 de la personne; ou

B.2.2.4.2 du parent ou tuteur légal lors d'un filtrage de sécurité pour des personnes de moins de 18 ans.

Absence de consentement ou d'information

B.2.2.5 Lorsqu'une personne ne donne pas son consentement, qu'elle le retire ou qu'elle ne fournit pas les renseignements requis pour le filtrage de sécurité, cesser les activités de filtrage et :

B.2.2.5.1 lorsque le filtrage de sécurité porte sur un filtrage de sécurité initial ou amélioré :

B.2.2.5.1.1 informer la personne que :

- a. le filtrage de sécurité ne peut avoir lieu sans le consentement ou les renseignements requis;
- b. le défaut de fournir le consentement et les renseignements requis aura pour effet que la personne concernée ne sera plus prise en considération pour la nomination, le poste, le contrat, l'affectation ou toute autre entente en question;

B.2.2.5.1.2 annuler le processus de filtrage pour des raisons administratives jusqu'à ce que le consentement et les renseignements requis soient obtenus;

B.2.2.5.1.3 aviser l'autorité contractante lorsque le filtrage de sécurité est mené à l'appui d'un contrat.

B.2.2.5.2 lorsque le filtrage de sécurité concerne une mise à jour :

B.2.2.5.2.1 informer et consulter le gestionnaire de la personne;

B.2.2.5.2.2 évaluer le risque associé au maintien en poste de la personne;

B.2.2.5.2.3 quand la personne ne fournit pas les renseignements requis, et que le filtrage de sécurité :

- a. ne peut être effectué en raison des renseignements manquants; ou
- b. ne peut être effectué avant l'expiration de la cote ou de l'autorisation; et
- c. présente un risque de sécurité inacceptable pour le ministère ou le gouvernement du Canada :

B.2.2.5.2.3.1 consulter la direction des ressources humaines ou informer l'autorité contractante;

B.2.2.5.2.3.2 suspendre la cote ou l'autorisation et entamer une révision pour motif valable; ou

B.2.2.5.2.4 lorsqu'une personne ne donne pas son consentement ou le retire :

B.2.2.5.2.4.1 documenter le refus de la personne et aviser cette dernière des conséquences

du défaut de fournir le
consentement;

B.2.2.5.2.4.2 suspendre la cote ou
l'autorisation de la
personne;

B.2.2.5.2.4.3 révoquer la cote ou
l'autorisation de la
personne 30 jours après la
suspension si le
consentement n'a toujours
pas été fourni.

Gestion des dossiers de filtrage de sécurité

B.2.2.6 Créer et tenir à jour un dossier pour chaque personne faisant
l'objet d'un filtrage de sécurité contenant des
renseignements personnels pertinents, notamment :

B.2.2.6.1 copies numériques ou papier original des
formulaire et des questionnaires sur le filtrage de
sécurité dûment remplis;

B.2.2.6.2 résultats pertinents de toutes les activités de
filtrage de sécurité, vérifications, enquêtes et
évaluations, tous datés;

B.2.2.6.3 analyse des résultats et de tout conseil ou toute
recommandation à l'appui de la prise de décisions;

B.2.2.6.4 décisions d'octroi, d'octroi sous conditions, de
refus, de révocation, de suspension en attendant
une enquête ou d'annulation pour des raisons
administratives d'une cote ou d'une autorisation
de sécurité;

B.2.2.6.5 renseignements pertinents liés aux conditions, à
l'accès temporaire, à la révision pour motif valable
ou à l'enquête, et à toute décision qui en découle.

B.2.2.7 Mettre à jour les dossiers de filtrage de sécurité dans les cas suivants :

- a. Un changement dans la situation personnelle de la personne est signalé, comprenant au moins un des éléments suivants :
 - i. changement de statut du casier judiciaire;
 - ii. démêlés avec la justice;
 - iii. association avec des criminels;
 - iv. changement significatif de la situation financière;
 - v. changements supplémentaires dans le statut personnel ou juridique d'une personne lorsqu'elle travaille pour une organisation de sécurité ou de renseignement.
- b. Un changement est apporté à la cote ou à l'autorisation de sécurité de la personne;
- c. La cote ou l'autorisation de sécurité de la personne est susceptible d'être revue pour un motif valable.
- d. Une décision est prise par rapport aux éléments ci-dessus.

B.2.2.8 Veiller à ce que les résultats d'enquêtes propres à un ministère, qui sont effectuées au moyen de sources de données et d'indices propres au ministère, soient uniquement inclus dans le dossier de filtrage de sécurité d'une personne lorsqu'ils sont utilisés pour dissiper un doute.

B.2.2.9 Retirer des dossiers de filtrage de sécurité les renseignements ayant trait aux actes criminels pour lesquels la personne a obtenu une suspension de son casier, et les éliminer.

Transfert des dossiers de filtrage de sécurité

B.2.2.10 Rendre le dossier de filtrage de sécurité de la personne accessible pour faciliter le mouvement temporaire ou définitif :

B.2.2.10.1 d'une personne au sein d'un ministère ou entre ministères;

B.2.2.10.2 d'un entrepreneur entre des contrats.

B.2.2.11 Transférer le dossier de filtrage de sécurité d'une personne :

B.2.2.11.1 sur demande et en temps opportun;

B.2.2.11.2 lorsqu'elle change définitivement de ministère;

B.2.2.11.3 conformément aux exigences relatives à la réactivation et à l'expiration;

B.2.2.11.4 sauf dans les situations suivantes :

B.2.2.11.4.1 toute évaluation de la sécurité classifiée du SCRS, qui doit être retournée au SCRS :

B.2.2.11.4.1.1 informer le dirigeant principal de la sécurité du ministère destinataire de l'existence de l'évaluation;

B.2.2.11.4.2 une inscription d'absolution obtenue en vertu de l'article 730 du *Code criminel* ne doit pas être :

- a. transféré à un autre ministère, y compris la reconnaissance de l'existence du dossier;
- b. divulgué, y compris le fait que l'absolution a eu lieu, à moins d'avoir reçu l'approbation préalable du

ministre de la Sécurité
publique si :

- i. plus d'un an
s'est écoulé
depuis
l'absolution
inconditionnelle
de la
personne;
- ii. plus de trois
ans se sont
écoulés depuis
que la
personne a
été absoute
selon les
conditions
prévues dans
l'ordonnance
de probation.

B.2.2.12 À la réception d'un dossier de filtrage de sécurité transféré :

B.2.2.12.1 mettre à jour les activités de filtrage de sécurité
lorsque :

- a. les résultats dépassent la période de
validité;
- b. des éléments de preuve donnent à
penser que le filtrage de sécurité n'a
pas été effectué auparavant
conformément à la présente
Directive;
- c. la cote ou l'autorisation a des
conditions;
- d. les résultats des vérifications du
casier judiciaire, des vérifications des
dossiers policier ou des évaluations

de la sécurité ont été retirés du dossier;

- e. le dossier contient des renseignements défavorables pouvant représenter un risque pour la sécurité du ministère destinataire;

B.2.2.12.2 consigner les raisons du refus de la cote ou de l'autorisation actuelle dans un dossier de filtrage de sécurité transféré, et reprendre le filtrage de sécurité de la personne.

B.2.2.13 Lors du transfert de l'autorisation de sécurité d'une personne, aviser le SCRS au moyen du formulaire 4160 – Avis de changement de l'autorisation de sécurité du SCRS.

Désactivation et réactivation

B.2.2.14 Désactiver une cote ou une autorisation de sécurité valide lorsque :

B.2.2.14.1 un employé :

- a. a pris sa retraite ou que son emploi a pris fin d'une autre manière,
- b. a pris un congé autorisé du gouvernement du Canada d'une durée supérieure à :
 - i. deux ans pour une cote;
 - ii. un an pour une autorisation;
- c. s'est absenté sans autorisation du gouvernement du Canada pendant plus de 30 jours;

B.2.2.14.2 un entrepreneur ou une autre personne a été exclu du contrat ou d'une autre entente; ou

B.2.2.14.3 le contrat ou l'autre entente est achevé, annulé ou résilié.

B.2.2.15 Réactiver la cote ou l'autorisation de sécurité :

B.2.2.15.1 uniquement si la période de validité initiale n'est pas terminée; et

B.2.2.15.2 si un employé redevient actif et n'a pas :

- a. passé plus de deux ans sans cote de sécurité valide;
- b. passé plus d'un an sans autorisation de sécurité valide; ou

B.2.2.15.3 si un entrepreneur ou une autre personne n'a pas :

- a. passé plus de deux ans sans cote de sécurité valide;
- b. passé plus d'un an sans autorisation de sécurité valide;
- c. passé plus d'un an sans cote ou autorisation d'accès au site valide.

B.2.2.16 Lors de la réactivation d'une cote ou d'une autorisation :

B.2.2.16.1 Revalider l'information confirmant l'identité.

B.2.2.16.2 Exiger que les personnes rendent compte de leurs activités pendant la période d'absence et des circonstances entourant leur départ.

B.2.2.16.3 Ne pas prolonger la période de validité.

B.2.2.16.4 Ne pas réactiver une cote ou une autorisation de sécurité et répéter le filtrage de sécurité dans les cas suivants :

B.2.2.16.4.1 les circonstances entourant le départ impliquent ce qui suit :

- a. révision pour motif valable;
- b. suspension en attente de l'issue d'une enquête;

- c. une résolution des doutes en suspens;
- d. motifs disciplinaires;

B.2.2.16.4.2 le dossier contient des renseignements ou des conditions défavorables.

B.2.2.16.4.3 La cote ou autorisation de sécurité a dépassé sa période de validité.

B.2.2.17 Annuler pour des raisons administratives une cote ou une autorisation de sécurité ou une autorisation d'accès à un site, une fois que la période de réactivation de la personne s'est écoulée et que le dossier est resté inactif.

Conservation et élimination des dossiers

B.2.2.18 Conserver les dossiers de filtrage de sécurité des personnes contenus dans :

B.2.2.18.1 le fichier de renseignements personnels ordinaires POU 917 (filtrage de sécurité), pendant au moins deux ans après le départ de la personne de la fonction publique fédérale :

B.2.2.18.1.1 empêcher que les dossiers de filtrage de sécurité des personnes qui ont quitté leur emploi au sein de la fonction publique fédérale soient transférés au Centre des documents du personnel du ministère ou à tout Centre de services régionaux de Bibliothèque et Archives Canada;

B.2.2.18.2 le fichier de renseignements personnels ordinaires POU 917 (filtrage de sécurité), pour ceux qui se sont vu refuser ou révoquer une cote ou une autorisation de sécurité pendant au moins 10 ans après leur départ de la fonction publique fédérale.

Annexe C. Procédures obligatoires quant aux activités de filtrage de sécurité

C.1 Date d'entrée en vigueur

C.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

C.2 Procédures

C.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes A.2.2.2.3, A.2.2.3, A.2.2.8.2 et A.2.2.9 de la Norme sur le modèle de filtrage de sécurité et l'analyse des postes.

C.2.2 Voici les procédures obligatoires :

C.2.2.1 Mener des activités de filtrage de sécurité conformément à l'annexe A1 et l'annexe A3 de l'annexe A – Norme sur le modèle de filtrage de sécurité et l'analyse des postes, tel qu'indiqué ci-dessous :

C.2.2.1.1 procéder à la vérification de l'identité avant d'entreprendre toute activité de filtrage de sécurité subséquente;

C.2.2.1.2 effectuer toutes les activités de filtrage de sécurité subséquentes relatives à la personne.

Pratiques de vérification de l'identité

C.2.2.1.3 Vérifier la preuve de l'identité conformément à la Norme sur l'assurance de l'identité et des justificatifs.

C.2.2.1.3.1 Appliquer le niveau 3 d'assurance de l'identité et des justificatifs comme niveau minimal requis pour tous les niveaux de filtrage de sécurité.

Pratiques de vérification des antécédents

C.2.2.1.4 Vérifier l'exactitude des renseignements sur les antécédents fournis par la personne en adoptant une approche fondée sur les risques.

C.2.2.1.4.1 Lorsqu'il n'est pas possible de vérifier les antécédents de toutes les années, envisager ce qui suit :

C.2.2.1.4.1.1 autres sources d'information, notamment :

C.2.2.1.4.1.1.1 références supplémentaires,

C.2.2.1.4.1.1.2 Résolution des doutes conformément à l'annexe E – Procédures obligatoires pour la résolution des doutes et la révision pour motif valable.

C.2.2.1.4.2 Tenir compte des personnes qui ont vécu hors du Canada pendant plus de six mois consécutifs au cours de la période requise par la cote ou l'autorisation de sécurité, de la manière suivante :

a. lettre de référence ou de recommandation d'une ambassade ou d'une mission étrangère au Canada;

- b. lettre de référence ou de recommandation d'une ambassade ou mission étrangère du Canada du pays où la personne a résidé;
- c. lettre de recommandation d'une université ou d'un établissement d'enseignement étranger;
- d. lettre ou certificat de police d'un organisme chargé de l'exécution de la loi du pays où la personne a résidé;
- e. sommaire de crédit provenant d'une institution financière étrangère reconnue;
- f. emploi ou affectation auprès d'un ministère ou d'un organisme du gouvernement du Canada ou des Forces armées canadiennes à l'étranger;
- g. renseignements provenant d'organisations homologues de filtrage de sécurité dans les pays avec lesquels le Canada a conclu des ententes bilatérales pour l'échange de renseignements sur le filtrage de sécurité;
- h. autres sources d'information qui sont suffisantes pour rendre

compte de leurs activités et du risque associé.

C.2.2.1.4.2.1 Évaluer les activités comptabilisées de l'une de ces manières en tenant compte du caractère adéquat et fiable de la source.

Vérification des diplômes et des désignations professionnelles

C.2.2.1.5 Vérifier les diplômes et les désignations professionnelles qui sont pertinents.

Vérification des références personnelles et professionnelles

C.2.2.1.6 Valider les renseignements sur la personne auprès des personnes qui la connaissent ou qui sont en mesure de la remarquer.

Enquête sur la situation financière

C.2.2.1.7 Obtenir le dossier de crédit à la consommation complet d'une agence d'évaluation du crédit qui :

C.2.2.1.7.1 comprend des renseignements sur les antécédents de crédit, les privilèges, les jugements ou la faillite de la personne;

C.2.2.1.7.2 exclut la cote de crédit de la personne et n'a pas d'incidence négative sur celle-ci.

C.2.2.1.8 Lorsqu'il n'est pas possible d'obtenir un dossier de crédit fiable auprès d'une agence d'évaluation du crédit, mettre au point un questionnaire d'enquête sur la situation financière que les personnes doivent remplir.

C.2.2.1.9 Appliquer les résultats de l'enquête sur la situation financière pour déterminer si une personne pose un risque de sécurité sur le fondement de pressions financières ou d'une mauvaise responsabilité financière par le passé.

Vérification du casier judiciaire

C.2.2.1.10 Procéder à une vérification du casier judiciaire dans le Répertoire national des casiers judiciaires de la Gendarmerie royale du Canada pour confirmer l'implication de la personne dans des activités criminelles.

C.2.2.1.11 Appliquer ce qui suit pour les personnes qui ont vécu hors du Canada pendant plus de six mois consécutifs au cours de la période requise par la cote ou l'autorisation de sécurité :

C.2.2.1.11.1 Obtenir un certificat de police ou un document équivalent qui fournit :

- a. un résumé du casier judiciaire de la personne;
- b. une déclaration de l'absence de tout casier judiciaire.

C.2.2.1.11.2 Lorsque pour un pays de résidence :

- a. aucun certificat de police ou document équivalent n'est fourni; ou
- b. l'obtention des documents présente un risque excessif pour la personne :

C.2.2.1.11.2.1 envisager d'autres sources d'information suffisantes pour :

C.2.2.1.11.2.1.1 confirmer
l'implication
ou la non-
implication
de la
personne
dans des
activités
criminelles,

C.2.2.1.11.2.1.2 évaluer le
risque
associé aux
condamnations
criminelles
antérieures.

C.2.2.1.12 Appliquer les résultats de la vérification du casier
judiciaire et des documents provenant de
l'étranger pour déterminer le risque associé aux
condamnations criminelles antérieures.

Évaluation de sécurité du SCRS

C.2.2.1.13 Obtenir une évaluation de sécurité du SCRS pour :

C.2.2.1.13.1 déterminer si les renseignements
disponibles sont suffisants pour
prendre une décision de filtrage de
sécurité;

C.2.2.1.13.2 évaluer, lorsque les renseignements
disponibles sont suffisants, s'il existe
des motifs raisonnables de croire que la
personne s'est livrée, se livre ou
pourrait se livrer à des activités qui
constituent une « menace envers la
sécurité du Canada » au sens de

Enquête sur Internet

C.2.2.1.14 Examiner les renseignements personnels accessibles au public sur Internet pour :

C.2.2.1.14.1 vérifier l'exactitude et l'intégrité des renseignements sur les antécédents fournis par la personne;

C.2.2.1.14.2 repérer les renseignements défavorables potentiels en fonction de comportements, de conduites, d'associations, de jugements ou de traits de caractère.

C.2.2.1.15 Prendre des mesures raisonnables pour vérifier l'exactitude des renseignements obtenus au moyen de l'enquête sur Internet.

Vérification des dossiers policier

C.2.2.1.16 Obtenir d'autres dossiers de la Gendarmerie royale du Canada et des corps policiers compétents pour confirmer :

C.2.2.1.16.1 l'existence de mandats non exécutés ou d'interdictions;

C.2.2.1.16.2 si la personne a des liens avec des activités criminelles ou liées au crime organisé.

Questionnaire de sécurité ou entrevue de sécurité

C.2.2.1.17 Mettre au point un questionnaire de sécurité devant être rempli ou une entrevue de sécurité sollicitant des renseignements pour :

C.2.2.1.17.1 repérer et valider les renseignements défavorables;

C.2.2.1.17.2 donner à la personne la possibilité d'expliquer les renseignements défavorables;

C.2.2.1.17.3 évaluer le risque de sécurité en fonction de l'idéologie, du comportement, des associations, du jugement, des traits de caractère et de la vulnérabilité à la coercition.

Test polygraphique

C.2.2.1.18 Effectuer un test polygraphique :

C.2.2.1.18.1 pour les postes qui nécessitent une autorisation de niveau Très secret approfondie;

C.2.2.1.18.1.1 ou lorsqu'il est nécessaire de se conformer aux accords internationaux d'échange de renseignements conclus par le gouvernement du Canada;

C.2.2.1.18.2 pour corroborer les résultats du filtrage de sécurité, y compris en l'absence de résultats.

Confirmation de la citoyenneté canadienne

C.2.2.1.19 Confirmer la citoyenneté canadienne pour une autorisation de sécurité de niveau Très secret ou Très secret approfondie;

C.2.2.1.19.1 conformément aux documents prescrits par le gouvernement du

Annexe D. Procédures obligatoires sur l'évaluation collective des activités de filtrage de sécurité

D.1 Date d'entrée en vigueur

D.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

D.2 Procédures

D.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.1.2 et 4.6.1 de la Directive sur le filtrage de sécurité.

D.2.2 Voici les procédures obligatoires.

Vérification de l'identité

D.2.2.1 Annuler le processus de filtrage de sécurité pour des raisons administratives lorsque l'information confirmant l'identité ne peut être vérifiée, malgré des efforts raisonnables et démontrables.

Vérification de la citoyenneté canadienne

D.2.2.2 Annuler la procédure de filtrage de sécurité pour des raisons administratives lorsque la citoyenneté canadienne ne peut être vérifiée, malgré des efforts raisonnables et démontrables, pour les autorisations de sécurité de niveau Très secret et Très secret approfondie.

Évaluation collective des activités de filtrage de sécurité

D.2.2.3 Évaluer de manière collective les résultats des activités de filtrage de sécurité.

D.2.2.3.1 S'appuyant sur :

D.2.2.3.1.1 la qualité, la quantité, la pertinence, la crédibilité et l'exhaustivité des renseignements disponibles relatifs au niveau de cote ou d'autorisation envisagé;

D.2.2.3.1.2 les facteurs contextuels associés au poste, au contrat ou à tout autre entente, y compris l'ensemble des renseignements relatifs à la personne;

D.2.2.3.1.3 la présence de renseignements défavorables et de renseignements obtenus à la suite d'une résolution des doutes, à considérer comme un facteur.

D.2.2.3.2 Évaluer :

D.2.2.3.2.1 la fiabilité d'une personne, y compris son honnêteté et la capacité d'y faire confiance pour :

- a. protéger les renseignements et les biens, y compris les installations et les systèmes de TI,
- b. ne pas abuser du niveau de confiance accordé,
- c. exécuter les tâches qui lui sont assignées d'une manière qui se reflétera de façon favorable sur le gouvernement du Canada,
- d. ne pas présenter de risque pour la sécurité du gouvernement du Canada;

D.2.2.3.2.2 la loyauté envers le Canada, le cas échéant, lorsqu'il existe des motifs

raisonnables de croire que :

a. la personne a pris part,
prend part, pourrait
prendre part ou pourrait
être incité à prendre part à
des activités qui
constituent une menace
envers la sécurité du
Canada d'après la
définition de cette notion
dans la *Loi sur le Service*
canadien du renseignement
de sécurité,

b. en matière de fiabilité qui
se rapporte à la loyauté :

i. la personne a
agi, agit,
pourrait agir
ou pourrait
être incitée à
agir d'une
manière qui
constitue une
menace
envers la
sécurité du
Canada;

ii. la personne a
communiqué,
pourrait
communiquer,
pourrait être
amenée à
communiquer
ou faire en
sorte que soit
communiquée

de
l'information
sensible d'une
manière
contraire à
l'intérêt
public.

D.2.2.3.2.2.1 Considérer la présence de renseignements qui soutien la probabilité de ces scénarios comme motif de refus d'une autorisation de sécurité ou d'une autorisation d'accès à un site.

D.2.2.3.2.2.2 Considérer l'absence de renseignements défavorables à la suite d'une évaluation de sécurité du SCRS comme un facteur favorable pour l'octroi d'une autorisation de sécurité ou d'une autorisation d'accès à un site.

D.2.2.3.2.2.3 Considérer l'insuffisance de renseignements fournis dans le cadre d'une évaluation de sécurité du SCRS comme un motif de refus d'une autorisation de sécurité ou d'une autorisation d'accès à un site.

Repérage et évaluation des renseignements défavorables

- D.2.2.4 Évaluer l'importance d'un renseignement défavorable à la lumière des détails se rattachant à ce renseignement et de l'ensemble des circonstances de la personne, notamment :
- a. les facteurs atténuants et aggravants;
 - b. la nature du renseignement défavorable;
 - c. la fréquence des renseignements défavorables;
 - d. les circonstances entourant les renseignements défavorables, notamment :
 - i. l'incidence des facteurs socio-économiques et culturels indiqués par la personne;
 - e. la gravité du renseignement défavorable;
 - f. le passage du temps;
 - g. les tâches à accomplir;
 - h. si la personne était ouverte et a volontairement fournit les renseignements;
 - i. les mesures correctives et les efforts de réadaptation de la personne.
- D.2.2.5 Lorsqu'une enquête sur Internet révèle des renseignements défavorables potentielles, avant de prendre une décision, il faut donner à la personne la possibilité :
- D.2.2.5.1 d'examiner un résumé des renseignements défavorables potentielles;
 - D.2.2.5.2 d'expliquer les renseignements.
- D.2.2.6 Refuser une cote ou une autorisation de sécurité à une personne qui ne peut pas occuper des fonctions publiques, passer un contrat ou recevoir des avantages au titre d'un contrat en vertu des paragraphes 750(2) et 750(3) du Code criminel.

Examen et communication des renseignements défavorables

- D.2.2.7 Examiner les renseignements défavorables en tant que motif pour procéder à une enquête plus approfondie, notamment

en vue de la tenue d'une entrevue de résolution des doutes.

- D.2.2.8 Lorsque la fonction de filtrage de sécurité concerne la prestation de services à des ministères clients, signaler les renseignements défavorables au dirigeant principal de la sécurité du ministère client qui envisage d'employer, de nommer ou d'affecter la personne ou de conclure un contrat ou un autre entente avec elle.

Annexe E. Procédures obligatoires pour la résolution des doutes et la révision pour motif valable

E.1. Date d'entrée en vigueur

- E.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

E.2 Procédures

- E.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.1.2, 4.1.1.1.3., 4.1.1.2 et 4.1.6 de la Directive sur le filtrage de sécurité.

- E.2.2 Voici les procédures obligatoires :

E.2.2.1 Démontrer et documenter que les renseignements défavorables et manquants ont été traités de manière approfondie;

E.2.2.2 Procéder à une résolution des doutes ou à une révision pour motif valable dans les plus brefs délais;

Résolution des doutes

E.2.2.3 Procéder à une résolution des doutes lorsque des renseignements invérifiables, manquants ou défavorables sont découverts au cours du filtrage de sécurité d'une personne.

E.2.2.4 Fournir à la personne un résumé des renseignements défavorables, manquants et invérifiables en question.

E.2.2.4.1 Avant de communiquer avec la personne :

E.2.2.4.1.1 consulter l'organisme d'enquête lorsque des renseignements défavorables sont découverts à la suite :

- a. d'une vérification des dossiers policier par la Gendarmerie royale du Canada,
- b. d'une évaluation de sécurité par le SCRS;

E.2.2.4.1.2 exclure les renseignements qui ne peuvent être communiqués :

- a. pour des raisons de sécurité nationale,
- b. car ils pourraient mettre en danger la sécurité d'autrui,
- c. car ils sont exemptés en vertu des articles 18, 19, 20 et 21 ainsi que des paragraphes 22(1) à 22(3) de la Loi sur la protection des renseignements personnels.

E.2.2.5 Mener des activités supplémentaires de filtrage de sécurité :

E.2.2.5.1 pour résoudre les doutes, lorsque des renseignements sont disponibles ou rapportés au sujet d'une personne et qu'ils peuvent mettre en doute sa fiabilité ou sa loyauté envers le Canada;

E.2.2.5.2 quand :

E.2.2.5.2.1 la personne fournit son consentement,

E.2.2.6 Avant qu'une décision ne soit prise, procéder à une entrevue de résolution des doutes afin de donner l'occasion à la personne concernée de discuter de tout sujet de préoccupation et d'expliquer la situation.

E.2.2.7 Examiner les renseignements obtenus dans le cadre d'une résolution des doutes concernant l'admissibilité d'une personne à une cote ou une autorisation de sécurité.

Révision pour motif valable

E.2.2.8 Procéder à une révision pour motif valable de la cote ou de l'autorisation de sécurité précédemment accordée à une personne dans les cas où :

E.2.2.8.1 des renseignements découverts ou rapportés au sujet de la personne pourraient remettre en question sa fiabilité ou sa loyauté envers le Canada; ou

E.2.2.8.2 les renseignements défavorables reflètent :

E.2.2.8.2.1 un jugement douteux ou de la malhonnêteté qui s'est produit récemment; ou

E.2.2.8.2.2 une tendance récurrente de jugement douteux ou de malhonnêteté.

E.2.2.9 Lors d'une révision pour motif valable, conformément au paragraphe F.2.2.11 de l'annexe F – Procédures obligatoires relatives aux mesures de sécurité lors de l'octroi de contrats et d'autres ententes, envisager la décision de suspendre :

E.2.2.9.1 une cote ou une autorisation de sécurité; ou

E.2.2.9.2 l'accès aux renseignements sensibles et aux biens, y compris les installations et les systèmes de TI.

E.2.2.10 Lancer le processus de révision pour motif valable sous la forme d'une enquête administrative comprenant une entrevue avec la personne concernée.

E.2.2.11 Lorsqu'une révision pour motif valable est menée parallèlement à une procédure disciplinaire à l'encontre d'un employé :

E.2.2.11.1 gérer les processus avec des décideurs distincts;

E.2.2.11.2 ne consigner une décision disciplinaire dans le dossier de sécurité que si elle est liée à un enjeu de sécurité.

E.2.2.11.3 consulter :

- a. la direction des ressources humaines du ministère,
- b. le Centre de droit du travail et de l'emploi, le cas échéant.

E.2.2.12 Examiner les renseignements obtenus dans le cadre d'une révision pour motif valable portant sur le maintien de l'admissibilité d'une personne à conserver une cote ou une autorisation de sécurité.

Annexe F. Procédures obligatoires pour les décisions et les avis en matière de filtrage de sécurité

F.1 Date d'entrée en vigueur

F.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

F.2 Procédures

F.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.3 et 4.6.1 de la Directive sur le filtrage de sécurité.

F.2.2 Voici les procédures obligatoires.

Décision d'octroi

F.2.2.1 Envisager une décision d'octroi lorsque l'évaluation collective des résultats du filtrage de sécurité d'une personne indique ce qui suit :

- a. Il n'existe aucun élément de preuve crédible mettant en doute la fiabilité de la personne et, le cas échéant, sa loyauté envers le Canada.
- b. Les renseignements défavorables découverts lors du filtrage de sécurité ont été traités.

F.2.2.2 Prendre la décision d'octroyer une cote ou autorisation de sécurité au moment du traitement du filtrage de sécurité.

Avis d'une décision d'octroi

F.2.2.3 Informer la personne de la décision d'accorder une cote ou autorisation de sécurité au moyen d'une séance d'information sur la sécurité.

Décision d'octroi sous conditions

F.2.2.4 Ne pas faire un octroi sous conditions comme substitut au filtrage de sécurité des personnes au niveau requis par le poste.

F.2.2.5 Envisager une décision d'octroi sous conditions uniquement :

- a. lorsque les conditions sont jugées suffisantes pour atténuer le risque de sécurité lié à l'octroi;
- b. lorsqu'il existe un besoin avéré d'embaucher la personne.

F.2.2.6 Imposer des conditions qui précisent officiellement les restrictions liées à l'octroi d'une cote ou autorisation de sécurité, notamment :

F.2.2.6.1 les limites d'accès aux renseignements et aux biens, y compris les installations et les systèmes de TI, qui sont nécessaires à l'exécution des tâches attribuées;

F.2.2.6.2 lorsqu'une ou plusieurs des conditions suivantes s'appliquent :

- a. ne pas accorder l'accès à des renseignements classifiés provenant d'un gouvernement étranger sans le consentement écrit de celui-ci, sous réserve des dispositions de toute entente sur la communication d'information,
- b. ne pas accorder l'accès à des renseignements classifiés provenant d'autres ministères sans consulter celui-ci,
- c. la cote ou l'autorisation de sécurité accordée à la personne n'est pas transférable à une autre fonction ou à un autre poste au sein du même ministère ou dans un autre ministère;

F.2.2.6.3 au besoin :

F.2.2.6.3.1 appliquer des exigences supplémentaires en matière de suivi et de rapports pour fournir une assurance supplémentaire de la fiabilité ou de la loyauté maintenue de la personne à l'égard du Canada,

F.2.2.6.3.2 limiter l'accès de la personne aux renseignements et aux biens, y compris les installations et les systèmes de TI, aux heures de travail désignées uniquement,

F.2.2.6.3.3 établir d'autres conditions raisonnables nécessaires pour gérer efficacement les risques liés à la sécurité du ministère ou du gouvernement du Canada.

F.2.2.7 Réévaluer les conditions de sécurité au moins une fois par an.

Avis d'une décision d'octroi sous conditions

F.2.2.8 Aviser la personne de la décision d'accorder une cote ou autorisation de sécurité soumise à des conditions au moyen d'une séance d'information sur la sécurité, en précisant la nature des conditions.

F.2.2.9 Obtenir une attestation de la personne comme quoi elle reconnaît ses responsabilités en matière de sécurité, notamment la nature des conditions.

F.2.2.10 Consigner la décision et l'attestation au dossier de filtrage de sécurité.

Décision de suspendre dans l'attente de l'issue d'une enquête

F.2.2.11 Envisager de suspendre une cote ou autorisation de sécurité dans les cas suivants :

- a. une enquête est en cours;
- b. les renseignements obtenus laissent entendre que la présence continue de la personne pourrait poser un risque de sécurité raisonnable pour autrui, le ministère ou le gouvernement du Canada;
 - i. d'autres modalités de travail ne suffisent pas à atténuer le risque lié à la sécurité,
 - ii. la présence continue de la personne pourrait compromettre ou entraver l'enquête.

F.2.2.12 Avant de prendre la décision de suspendre une cote ou autorisation de sécurité :

F.2.2.12.1 pour un employé :

F.2.2.12.1.1 consulter la direction des ressources humaines pour veiller à ce que les

obligations de l'employeur en matière de relations de travail soient prises en compte et respectées.

F.2.2.12.2 pour un entrepreneur ou une autre personne :

F.2.2.12.2.1 aviser l'autorité contractante avant l'entrepreneur.

Avis d'une décision de suspension

F.2.2.13 Aviser la personne par écrit des mesures à entreprendre, y compris des éléments suivants :

- a. la décision de suspendre la cote ou autorisation de sécurité en attendant une enquête;
- b. les raisons pour lesquelles la cote ou autorisation de sécurité est suspendue;
- c. toute circonstance ou tout facteur contributif pris en considération pour en arriver à cette décision;
- d. les modalités et le calendrier d'application de la suspension;
- e. la manière dont la personne peut se prévaloir de son droit de répondre à la mesure ou de la contester.

Décision de rétablissement à la suite d'une suspension

F.2.2.14 Si une cote ou autorisation de sécurité a été suspendue pour un motif valable :

F.2.2.14.1 au cours d'une enquête, envisager la possibilité d'un rétablissement :

- a. lorsque de nouveaux faits ou de nouvelles circonstances sont repérés;
et
- b. dans un délai raisonnable et périodiquement tout au long de la suspension.

F.2.2.14.2 prendre une décision de rétablir ou de révoquer sur la base de ce qui suit :

- a. des conclusions et des recommandations de l'enquête; et
- b. le nouveau risque pour le ministère ou le gouvernement du Canada.

Avis d'une décision de rétablissement à la suite d'une suspension

F.2.2.15 Informer l'employé de la décision de rétablir la cote ou autorisation de sécurité au moyen d'une séance d'information sur la sécurité.

Décision de refus

F.2.2.16 Envisager une décision de refus lorsqu'il existe des éléments de preuve crédibles qui jettent un doute sur les capacités d'une personne :

- a. à être fiable et, le cas échéant, loyale envers le Canada;
- b. à protéger les biens et les renseignements sensibles, y compris les installations et les systèmes de TI.

F.2.2.17 Aviser l'administrateur général de la décision de refuser une autorisation de sécurité dans les cinq jours suivant la prise de décision.

Décision de révocation

F.2.2.18 Envisager une décision de révocation :

F.2.2.18.1 à la suite d'une mise à jour, d'une revue à la hausse ou d'une révision pour motif valable de la cote ou autorisation de sécurité précédemment accordée à une personne;

F.2.2.18.2 lorsqu'il existe des éléments de preuve crédibles qui jettent un doute sur la capacité d'une personne :

- a. à être fiable et, le cas échéant, loyale envers le Canada,
- b. à protéger les biens et les renseignements sensibles, y compris les installations et les systèmes de TI.

F.2.2.19 Avant de rendre une décision de révocation :

F.2.2.19.1 procéder à un examen afin de déterminer s'il existe d'autres options viables, y compris abaisser la cote ou l'autorisation d'une personne;

F.2.2.19.2 pour un employé :

F.2.2.19.2.1 consulter la direction des ressources humaines pour veiller à ce que les obligations de l'employeur en matière de relations de travail soient prises en compte et respectées;

F.2.2.19.3 pour un entrepreneur ou une autre personne :

F.2.2.19.3.1 aviser l'autorité contractante avant l'entrepreneur;

F.2.2.19.4 consulter l'administrateur général en cas de litige quant aux mesures à prendre.

F.2.2.20 À la suite d'une décision de révocation :

F.2.2.20.1 Avant d'informer la personne concernée, veiller à ce que des mesures soient prises pour l'empêcher d'accéder à des biens et à des renseignements sensibles, y compris les installations et les systèmes de TI.

F.2.2.20.2 Informer l'administrateur général de la décision de révoquer une autorisation de sécurité dans les cinq jours suivant la prise de décision.

F.2.2.20.3 Pour un entrepreneur, aviser l'autorité contractante avant l'entrepreneur.

F.2.2.20.4 Aviser le SCRS au moyen du formulaire SCRS 4160 – Avis de changement de l'autorisation de sécurité.

Avis d'une décision de refus ou de révocation

F.2.2.21 Informer la personne de la décision de refuser ou de révoquer sa cote ou autorisation de sécurité :

F.2.2.21.1 dans les dix jours suivant la prise de la décision;

F.2.2.21.2 par écrit au nom du dirigeant principal de la sécurité ou de l'administrateur général;

F.2.2.21.3 inclure les raisons de la décision et les renseignements sur lesquels la décision repose :

F.2.2.21.3.1 exclure les renseignements qui ne peuvent être communiqués :

a. en vertu de la Loi sur la protection des

renseignements privés,

b. pour des raisons de sécurité nationale,

c. dans le cadre d'autres législations fédérales;

F.2.2.21.4 informer la personne de ses droits de révision ou de recours.

F.2.2.22 Après avoir avisé la personne concernée, informer le SCRS de la décision de refuser ou de révoquer une autorisation de sécurité.

Annexe G. Procédures obligatoires relatives à l'octroi, au maintien et à l'assurance du

filtrage de sécurité d'une personne

G.1 Date d'entrée en vigueur

G.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

G.1.2 Ces procédures remplacent l'annexe F – Suivi de la Norme sur le filtrage de sécurité datant du 20 octobre 2014.

G.2 Procédures

G.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1 et 4.6.1 de la Directive sur le filtrage de sécurité.

G.2.2 Le dirigeant principal de la sécurité et les personnes exerçant des responsabilités subordonnées doivent suivre les procédures obligatoires qui suivent :

Séance d'information sur la sécurité

G.2.2.1 La séance d'information sur la sécurité doit :

G.2.2.1.1 mobiliser le gestionnaire de la personne ou les responsables de sécurité;

G.2.2.1.2 informer la personne de ses responsabilités au titre de la Politique sur la sécurité du gouvernement, notamment :

- a. les autorisations d'accès de son niveau de filtrage,
- b. les attentes en matière de sécurité liées à son poste, à son contrat ou à tout autre entente,
- c. le partage des responsabilités en matière de sécurité au sein de l'organisation;

G.2.2.1.3 être tenue avant que la personne ait accès à des biens et à des renseignements sensibles, y compris les installations et les systèmes de TI;

G.2.2.1.4 être tenue dans ces circonstances :

- a. à la suite d'une décision d'octroi ou d'octroi avec conditions,
- b. à chaque changement du niveau de filtrage de sécurité d'une personne,
- c. si nécessaire, en fonction du cycle de mise à jour défini à l'annexe G2 et à l'annexe G3,
- d. à la demande du ministère selon son environnement de risque de sécurité;

G.2.2.1.5 Donner à la personne la possibilité de poser des questions.

G.2.2.1.6 Inclure la signature du Certificat d'enquête de sécurité et profil de sécurité par la personne.

G.2.2.1.6.1 Conserver le document dans le dossier de filtrage de sécurité de la personne.

G.2.2.2 Lorsqu'une autorisation de sécurité est accordée, informer le SCRS au moyen de son formulaire 4195 – Avis d'autorisation de sécurité.

Sensibilisation à la sécurité

G.2.2.3 Mener des séances de sensibilisation à la sécurité conformément à l'annexe H – Procédures obligatoires relatives aux mesures de sécurité dans la sensibilisation et la formation de la Directive sur la gestion de la sécurité, au minimum à la suite d'octroi et de mise à jour dans le cycle de vie du filtrage de sécurité.

G.2.2.3.1 Informer les personnes de l'obligation de signaler tout changement de leur situation personnelle, notamment :

- a. changement de statut du casier judiciaire;
- b. démêlés avec la justice;
- c. association avec des criminels;

d. changement significatif de la situation financière.

- G.2.2.3.2 Informer les personnes qui travaillent dans le domaine de la sécurité ou du renseignement de l'obligation de signaler tout autre changement dans leur statut personnel ou juridique, y compris un changement d'état civil.
- G.2.2.3.3 Indiquer aux gestionnaires la façon de signaler les changements de comportement observés chez les personnes sous leur responsabilité, et à qui le signaler.

Activités récurrentes

- G.2.2.4 Passer en revue les exigences en matière de filtrage de sécurité pour les postes lors de la mise en œuvre de nouveaux programmes ou activités ou de la modification importante de programmes et activités existants, et au minimum tous les cinq ans.
 - G.2.2.4.1 Informer les fournisseurs de services de filtrage de sécurité de tout changement aux exigences.
- G.2.2.5 Mener des activités de filtrage de sécurité pour les dossiers de filtrage de sécurité du personnel qui répondent aux fréquences minimales prescrites à l'annexe G1.

Mise à jour

- G.2.2.6 Procéder à la mise à jour du filtrage de sécurité de la personne avant la fin de la période de validité, en plus des activités récurrentes.
- G.2.2.7 Réexaminer la fiabilité ou la loyauté de la personne depuis qu'elle a obtenu sa dernière cote ou autorisation de sécurité.
 - G.2.2.7.1 Mener le processus de mise à jour conformément à ce qui suit :

G.2.2.7.1.1 cycles de mise à jour du filtrage de sécurité et activités indiquées à l'annexe G2;

G.2.2.7.1.2 cycles de mise à jour du contrôle d'accès aux sites et activités indiquées à l'annexe G3.

G.2.2.7.2 Évaluer si des changements dans la situation personnelle constituent un risque lié à la sécurité.

G.2.2.7.3 Déterminer le maintien de l'admissibilité de la personne à une cote ou autorisation de sécurité, selon l'évaluation collective des activités de filtrage de sécurité.

G.2.2.7.4 Tenir une séance d'information sur la sécurité pour informer la personne de ses responsabilités en matière de sécurité au titre des paragraphes G.2.2.1 et G.2.2.3.

G.2.2.8 Lorsqu'une personne ne donne pas son consentement, le retire ou ne fournit pas les renseignements requis, il convient de procéder conformément au paragraphe B.2.2.6.2 de l'annexe B – Procédures obligatoires pour la gestion des renseignements personnels aux fins de filtrage de sécurité.

G.2.2.9 Répéter toute activité de filtrage de sécurité :

G.2.2.9.1 lorsque requis par le cycle de mise à jour;

G.2.2.9.2 lorsqu'il y a des raisons de croire que :

- a. les activités n'ont pas été menées correctement,
- b. le dossier ne contient aucun document sur la tenue initiale des activités de contrôle.

Revue à la hausse

G.2.2.10 Lors d'une revue à la hausse d'une cote ou autorisation de sécurité valide :

G.2.2.10.1 Mener des activités supplémentaires de filtrage de sécurité et respecter le nombre d'années de renseignements sur les antécédents requises pour le nouveau niveau conformément à l'annexe A1 de l'annexe A – Norme sur le modèle de filtrage de sécurité et l'analyse des postes.

G.2.2.10.2 Déterminer l'admissibilité d'une personne à détenir une nouvelle cote ou autorisation de sécurité, en fonction des résultats collectifs de toutes les activités de filtrage de sécurité.

G.2.2.10.3 détenir une séance d'information sur la sécurité pour informer la personne de ses responsabilités en matière de sécurité au titre des paragraphes G.2.2.1 et G.2.2.3.

G.2.2.11 Lorsqu'une personne ne donne pas son consentement, le retire ou ne fournit pas les renseignements requis, il convient de procéder conformément au paragraphe B.2.2.6.1 de l'annexe B – Procédures obligatoires pour la gestion des renseignements personnels aux fins de filtrage de sécurité.

Déclassements

G.2.2.12 Lors du déclassement d'une cote ou d'une autorisation valide à un niveau inférieur :

G.2.2.12.1 Tenir une séance d'information sur la sécurité pour informer la personne de ses responsabilités en matière de sécurité au titre des paragraphes G.2.2.1 et G.2.2.3;

G.2.2.12.1.1 Il s'agit notamment d'informer les personnes et les gestionnaires que la personne ne peut plus accéder à des niveaux supérieurs de biens et de

renseignements sensibles, notamment les installations et les systèmes de TI.

Séances de compte rendu sur la sécurité

G.2.2.13 Les séances de compte rendu sur la sécurité doivent :

G.2.2.13.1 être fournies aux personnes avant la fin de leur emploi ou de leur embauche auprès du ministère;

G.2.2.13.2 informer les personnes de leurs responsabilités continues à l'égard du maintien de la confidentialité des renseignements sensibles auxquels elles avaient accès;

G.2.2.13.3 s'appuyer sur le Certificat d'enquête de sécurité et profil de sécurité pour consigner :

- a. la tenue de la séance de compte rendu,
- b. lorsqu'il est impossible de tenir la séance de compte rendu avec la personne.

G.2.2.13.3.1 À conserver dans le dossier de filtrage de sécurité de la personne conformément au paragraphe B.2.2.18 de l'annexe B : Procédures obligatoires pour la gestion des renseignements personnels aux fins de filtrage de sécurité.

Annexe G1. Fréquence minimale de la mise à jour périodique des activités de filtrage de sécurité

Activités de filtrage de sécurité	Fréquence minimale	Activités de filtrage de sécurité	Fréquence minimale
-----------------------------------	--------------------	-----------------------------------	--------------------

Cote de fiabilité • Aucune	Sans objet	Cote de fiabilité approfondie • Enquête sur la situation financière • Vérification du casier judiciaire • Enquête sur Internet	5 ans
Autorisation de niveau Secret • Enquête sur la situation financière • Vérification du casier judiciaire	5 ans	Autorisation de niveau Secret approfondie • Enquête sur la situation financière • Vérification du casier judiciaire • Enquête sur Internet	5 ans
Autorisation de niveau Très secret • Enquête sur la situation financière • Vérification du casier judiciaire • Enquête sur Internet	3 ans	Autorisation de niveau Très secret approfondie • Enquête sur la situation financière • Vérification du casier judiciaire • Enquête sur Internet	1 an

Annexe G2. Activités de filtrage de sécurité et exigences minimales de mise à jour connexes

Activités de filtrage de sécurité	Exigence de mise à jour	Activités de filtrage de sécurité	Exigence de mise à jour

Cote de fiabilité • Formulaire de demande mis à jour couvrant la période depuis la dernière mise à jour • Enquête sur la situation financière • Vérification du casier judiciaire	10 ans	Cote de fiabilité approfondie : Ensemble des activités pour la cote de fiabilité ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité	10 ans
Autorisation de niveau Secret Ensemble des activités pour la cote de fiabilité ainsi que : • Évaluation de sécurité du SCRS	10 ans	Autorisation de niveau Secret approfondie Ensemble des activités pour la cote de sécurité de niveau secret ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité	10 ans

Autorisation de niveau Très secret Ensemble des activités pour la cote de sécurité de niveau Secret ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité • Voyages à l'étranger, biens à l'étranger, références morales, études, service militaire	5 ans	Autorisation de niveau Très secret approfondie Ensemble des activités pour la cote de sécurité de niveau Très secret ainsi que : • Test polygraphique	5 ans
--	-------	---	-------

Annexe G3. Activités de contrôle de l'accès aux sites et exigences de mise à jour connexes

Activités de contrôle d'accès aux sites	Exigence de mise à jour
Autorisation de l'accès aux sites • Formulaire de demande mis à jour couvrant la période depuis la dernière mise à jour • Vérification du casier judiciaire	10 ans : peut être mis à jour plus souvent lorsque l'emploi, l'embauche, l'affectation, le contrat ou l'entente a pris fin depuis 12 mois ou plus.
Autorisation d'accès aux sites Toutes les activités relatives à la cote d'accès aux sites ainsi que : • Évaluation de sécurité du SCRS	10 ans : peut être mis à jour plus souvent lorsque l'emploi, l'embauche, l'affectation, le contrat ou l'entente a pris fin depuis 12 mois ou plus.

Activités supplémentaires Peuvent être utilisées conformément au paragraphe A.2.2.10 – Analyse des postes des non-employés. Ensemble des activités liées au contrôle d'accès aux sites ainsi que : • Enquête sur Internet • Vérification des dossiers policier • Questionnaire de sécurité ou entrevue de sécurité • Test polygraphique	10 ans : peut être mis à jour plus souvent lorsque l'emploi, l'embauche, l'affectation, le contrat ou l'entente a pris fin depuis 12 mois ou plus.
--	---

Annexe H. Procédures obligatoires pour aviser les personnes de leurs droits de révision et de recours

H.1 Date d'entrée en vigueur

H.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

H.2 Procédures

H.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.1.4, 4.2.2.5 et 4.6.1 de la Directive sur le filtrage de sécurité.

H.2.2 Voici les procédures obligatoires.

Exigences en matière d'avis de recours

H.2.2.1 Lors de la préparation des renseignements destinés à la personne, indiquer les mécanismes de révision et de recours pertinents en consultation avec :

- la direction des ressources humaines;
- les services juridiques des ministères;
- le Centre de droit du travail et de l'emploi.

H.2.2.2 Informer la personne par écrit de ses droits de révision et de recours en cas de refus, de révocation ou de suspension d'une cote ou autorisation de sécurité :

H.2.2.2.1 dans les 10 jours ouvrables suivant la prise de décision;

H.2.2.2.2 en indiquant les mécanismes de révision et de recours pertinents qui sont à sa disposition;

H.2.2.2.3 en consignant et en conservant la preuve de la communication de ces renseignements à la personne.

Annexe I. Procédures obligatoires pour les dirigeants principaux de la sécurité aux fins de gestion de l'accès temporaire à des biens ou des renseignements sensibles

I.1 Date d'entrée en vigueur

I.1.1 Les présentes procédures entrent en vigueur le 6 janvier 2025.

I.2 Procédures

I.2.1 Les présentes procédures fournissent des renseignements sur les exigences énoncées aux paragraphes 4.1.1.2 et 4.6.1 de la Directive sur le filtrage de sécurité.

I.2.2 Les procédures obligatoires pour les dirigeants principaux de la sécurité sont les suivantes :

Décision d'accorder un accès temporaire à des biens ou des renseignements sensibles

I.2.2.1 Ne pas envisager d'accorder un accès temporaire lorsque l'on s'attend à ce que l'accès soit nécessaire pendant plus de quatre mois.

- I.2.2.2 Ne pas envisager d'accorder un accès temporaire comme solution de rechange au filtrage de sécurité des personnes au niveau requis par le poste.
- I.2.2.3 Envisager d'accorder un accès temporaire à des biens et des renseignements sensibles, y compris à des installations ou des systèmes de TI, à la personne :
 - I.2.2.3.1 lorsqu'il existe un besoin opérationnel pour cette personne qui ne peut être satisfait par une autre personne disposant d'une autorisation de sécurité valide au niveau requis;
 - I.2.2.3.2 lorsqu'une évaluation des risques démontre que la nécessité d'accorder à la personne un accès temporaire l'emporte sur le risque associé à l'octroi de cet accès.
- I.2.2.4 Imposer des restrictions qui détaillent les limites d'accès aux biens et aux renseignements sensibles, y compris les installations ou les systèmes de TI touchés par les dispositions de l'accès temporaire.

Avis de la décision d'accorder un accès temporaire

- I.2.2.5 Aviser la personne de la décision de lui accorder un accès temporaire à des biens et à des renseignements sensibles, y compris des installations et des systèmes de TI, au moyen d'une séance d'information sur la sécurité. Mentionner notamment :
 - I.2.2.5.1 la durée de l'accès;
 - I.2.2.5.2 les dispositions de l'accès.
- I.2.2.6 Pour l'entente d'accès temporaire :
 - I.2.2.6.1 obtenir la signature de la personne qui reçoit l'accès;

- I.2.2.6.2 obtenir la signature du dépositaire des renseignements visés;
- I.2.2.6.3 signer l'entente;
- I.2.2.6.4 inclure l'entente dans le dossier de filtrage de sécurité de la personne.

Avis d'une décision de suppression de l'accès temporaire

I.2.2.7 Tenir une séance d'information avec la personne après le retrait de l'accès temporaire. Notamment :

- I.2.2.7.1 informer la personne de ses responsabilités continues à l'égard du maintien de la confidentialité des renseignements sensibles auxquels elle avait accès;
- I.2.2.7.2 inclure une copie de l'entente signé dans le dossier de filtrage de sécurité de la personne;
- I.2.2.7.3 conserver la preuve de la séance d'information dans le dossier de filtrage de sécurité de la personne.

Gestion de l'accès temporaire de la personne

I.2.2.8 Lorsque l'accès temporaire est accordé :

- I.2.2.8.1 Empêcher la personne d'accéder aux renseignements ou aux documents suivants :
 - a. renseignements compartimentés;
 - b. renseignements de niveau Très secret approfondi;
 - c. renseignements Protégé C;
 - d. renseignements pour lesquels l'accès est restreint conformément aux accords internationaux ou aux restrictions spéciales;
 - e. documents au Cabinet tels que définis par le gouvernement du Canada, le

Bureau du Conseil privé ou la
Politique sur la sécurité des
documents confidentiels du Cabinet;
f. renseignements sensibles provenant
d'autres gouvernements et ordres de
gouvernement;
g. renseignements, biens, installations
et systèmes de TI sensibles provenant
d'autres ministères sans approbation
consignée.

I.2.2.8.2 Assurer un contrôle intégral de l'accès aux biens et
aux renseignements sensibles, y compris les
installations et les systèmes de TI touchés par les
dispositions de l'accès temporaire.

Date modified: 2025-01-07