Service de sécurité géré du gouvernement du Canada (SSGGC)

Annexe A – Appendice A : Exigences de sécurité

Date: 8 juin 2012

1. Autres exigences de sécurité opérationnelle

Numéro	Nom	Définition
T11	PROTECTION DES SECRETS PARTAGÉS	Le service DOIT protéger les **secrets partagés** et le **mot de passe** en s'assurant que : 1. l'accès aux **secrets partagés** et aux mots de passe, sous format haché, est assujetti à des mesures de contrôle discrétionnaires qui n'en permettent l'accès qu'aux rôles et applications ayant besoin d'un tel accès.
T12	PROTECTION DES SECRETS PARTAGÉS	Le service DOIT protéger les **secrets partagés** à l'aide de la méthode suivante : a. la concaténation des **secrets partagés** avec un sel et (ou) un nom d'utilisateur qui sont par la suite hachés à l'aide d'un algorithme approuvé, de sorte que les calculs effectués rendent impossibles la réalisation d'attaques par dictionnaire ou par épuisement contre un fichier volé contenant les secrets partagés. Aux fins de la présente exigence, l'expression « algorithme approuvé » renvoie aux algorithmes approuvés par le CSTC, selon la version la plus récente du document publié sous le titre *Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements désignés PROTÉGÉ et pour les applications d'authentification et d'autorisation électroniques au sein du gouvernement du Canada* (ITSA-11D).
T13	PROTECTION DU MOT DE PASSE	Le service DOIT protéger le **mot de passe** de l'utilisateur final à l'aide de la méthode suivante : b. la concaténation du **mot de passe** avec un sel et (ou) un nom d'utilisateur qui est par la suite haché à l'aide d'un algorithme approuvé, de sorte que les calculs effectués rendent impossible la réalisation d'attaques par dictionnaire ou par épuisement contre un fichier volé contenant le mot de passe. Aux fins de la présente exigence, l'expression « algorithme approuvé » renvoie aux algorithmes approuvés par le CSTC, selon la version la plus récente du document publié sous le titre *Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements désignés PROTÉGÉ et pour les applications d'authentification et d'autorisation électroniques au sein du gouvernement du Canada* (ITSA-11D).

2. Contrôles de sécurité pour l'infrastructure

Le tableau qui suit présente les exigences de contrôle de sécurité s'appliquant à l'infrastructure des systèmes d'information relatifs au service ADSGC de l'entrepreneur. Ces contrôles sont tirés de l'annexe 3 du document ITSG-33 du *Catalogue des contrôles de sécurité* fourni à l'Annexe A - Appendice D : Catalogue des contrôles de sécurité – ITSG-33 Annexe 3 – version provisoire 3.1. Le terme « organisation » s'applique à l'entrepreneur, et l'expression « utilisateur organisationnel », au personnel de l'entrepreneur.

Numéro	Nom	Définition	Affectation
AC-1	POLITIQUE ET PROCÉDURES DE CONTRÔLE D'ACCÈS	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de contrôle d'accès formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité. (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de contrôle d'accès et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
AC-2	GESTION DES COMPTES	(A) L'organisation assure la gestion des comptes de système d'information, incluant : (A) L'identification des types de compte (c.-à-d., comptes individuels, de groupe, de système, d'application, d'invités/anonymes et temporaires). (B) L'organisation assure la gestion des comptes de système d'information, incluant l'établissement des conditions d'appartenance à un groupe. (C) L'identification des utilisateurs autorisés et l'établissement des privilèges d'accès. (D) L'exigence d'approbations appropriées pour les demandes d'établissement des comptes. (E) L'établissement, l'activation, la modification, la désactivation et la suppression de comptes. (F) L'autorisation et la surveillance spécifiques de l'utilisation des comptes d'invités/anonymes et temporaires. (G) Le signalement, aux gestionnaires de comptes, des comptes temporaires qui ne sont plus requis, du départ ou du transfert d'utilisateurs, ou des changements apportés à l'utilisation du système ou au besoin de connaître et (ou) de partager l'information. (H) La désactivation (i) des comptes temporaires qui ne sont plus requis et (ii) des comptes d'utilisateurs transférés qui ont quitté le GC. (I) L'octroi de droit d'accès au système basé sur (i) une autorisation d'accès valable, (ii) une utilisation prévue et (iii) d'autres attributs exigés par l'organisation ou associés à des fonctions liées à la mission et (ou) aux opérations. (J) L'examen des comptes [Affectation : fréquence définie par l'organisation].	(J) fréquence [à une fréquence ne dépassant pas une fois par mois]
AC-2.1	GESTION DES COMPTES	L'organisation utilise des mécanismes automatisés pour appuyer la gestion des comptes de système.	

Numéro	Nom	Définition	Affectation
AC-2.2	GESTION DES COMPTES	Le système annule automatiquement les comptes temporaires et d'urgence après [Affectation : durée définie par l'organisation pour chaque type de compte].	(2) Période de temps [ne dépassant pas 72 heures]
AC-2.3	GESTION DES COMPTES	Le système désactive automatiquement les comptes inactifs après [Affectation : durée définie par l'organisation].	(3) Période de temps [ne dépassant pas 30 jours]
AC-2.4	GESTION DES COMPTES	Le système vérifie automatiquement la création, la modification et la désactivation des comptes et les actions de cessation d'emploi, et en informe les personnes concernées, le cas échéant.	
AC-2.5	GESTION DES COMPTES	L'organisation : (a) Exige des utilisateurs qu'ils se déconnectent après [Affectation : durée d'inactivité prévue et (ou) description du moment de la déconnexion définies par l'organisation]; (b) Détermine la durée d'utilisation (incluant l'heure de la journée) des comptes; (c) Surveille toute utilisation atypique des comptes; et (d) Signale toute utilisation atypique aux agents désignés de l'organisation.	(5a) Période de temps [fin du jour ouvrable]
AC-2.7	GESTION DES COMPTES	L'organisation : (a) Établit et administre les comptes d'utilisateur privilégiés en conformité avec un schéma d'accès axé sur les rôles qui définit sous forme de rôles les privilèges associés au système et au réseau; et (b) Piste et surveille les attributions de rôles privilégiés.	
AC-3	APPLICATION DES DROITS D'ACCÈS	(A) Le système d'information applique les autorisations d'accès logique approuvées en conformité avec la politique concernée.	
AC-3.2	APPLICATION DES DROITS D'ACCÈS	Le système applique une double autorisation basée sur les politiques et procédures organisationnelles concernant [Affectation : commandes privilégiées définies par l'organisation].	Peut comprendre des activités de gestion de l'ICP.
AC-3.4	APPLICATION DES DROITS D'ACCÈS	Le système applique une politique de contrôle d'accès discrétionnaire (DAC) qui : (a) Permet aux utilisateurs de préciser et de contrôler le partage d'information soit avec des individus ou des groupes d'individus identifiés, ou les deux; (b) Limite la propagation des droits d'accès; et (c) Inclut ou exclut l'accès à la granularité d'un seul utilisateur.	
AC-4	APPLICATION DES CONTRÔLES DE FLUX D'INFORMATION	(A) Le système d'information recourt à des autorisations formelles de contrôle des flux d'information dans le système et entre les systèmes interconnectés, en conformité avec la politique concernée.	
AC-5	SÉPARATION DES TÂCHES	(A) L'organisation procède au besoin à la séparation des tâches des individus pour empêcher toute activité malveillante sans collusion. (B) L'organisation documente la séparation des tâches. (C) L'organisation applique la séparation des tâches en attribuant des autorisations d'accès aux systèmes d'information.	

Numéro	Nom	Définition	Affectation
AC-6	PRIVILÈGE MINIMUM	(A) L'organisation utilise le concept de privilège minimum et accorde un accès autorisé uniquement aux utilisateurs (et aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées en conformité avec les missions et les fonctions opérationnelles de l'organisation.	
AC-6.1	PRIVILÈGE MINIMUM	L'organisation autorise l'accès explicitement aux [Affectation : liste définie par l'organisation des fonctions de sécurité (déployées dans le matériel, le logiciel et le micrologiciel) et information sur la sécurité].	
AC-6.2	PRIVILÈGE MINIMUM	L'organisation exige des utilisateurs de comptes ou de rôles de système d'information, qui ont accès aux [Affectation : liste définie par l'organisation des fonctions de sécurité et information sur la sécurité], qu'ils utilisent des comptes ou des rôles non privilégiés pour accéder aux autres fonctions de système et, dans la mesure du possible, vérifient toute utilisation de comptes ou de rôles privilégiés pour ces fonctions.	
AC-6.5	PRIVILÈGE MINIMUM	L'organisation limite au personnel d'administration de système désigné l'autorisation d'utiliser les comptes de super utilisateur du système d'information.	
AC-7	TENTATIVES DE CONNEXION NON RÉUSSIES	(A) Le système d'information applique une limite de [Affectation : nombre défini par l'organisation] tentatives de connexion infructueuses consécutives par l'utilisateur sur une période de [Affectation : durée définie par l'organisation]. (B) Le système d'information [Sélection : verrouille le compte et (ou) le nœud pendant [Affectation : durée définie par l'organisation]; verrouille le compte et (ou) le nœud jusqu'à ce qu'un administrateur le libère; reporte le message de connexion suivant à [Affectation : algorithme de temporisation défini par l'organisation] automatiquement lorsque le nombre maximal de tentatives infructueuses est dépassé. Le contrôle s'applique tant à une connexion locale qu'à une connexion réseau.	(A) Nombre [d'un maximum de 3] (A) Période de temps [durée d'au moins 5 minutes] (B) Réponse automatique [verrouille le compte/nœud pendant au moins 5 minutes]
AC-7.1	TENTATIVES DE CONNEXION NON RÉUSSIES	Le système verrouille automatiquement le compte et (ou) nœud jusqu'à ce qu'il soit libéré par un administrateur lorsque le nombre maximal de tentatives infructueuses est dépassé.	
AC-8	AVIS CONCERNANT L'UTILISATION DU SYSTÈME	(A) Le système d'information, avant d'accorder l'accès, affiche un message approuvé ou une bannière d'avis concernant l'utilisation du système, qui inclut des avis de confidentialité et de sécurité en conformité avec la Politique d'utilisation des réseaux électroniques du SCT [Référence 6]. (B) Le système d'information maintient l'affichage du message ou de la bannière d'avis jusqu'à ce que les utilisateurs décident de se connecter ou d'accéder au système. (C) Le système d'information, dans le cas d'un système accessible au public, (i) affiche, le cas échéant, l'information d'utilisation avant d'accorder l'accès, (ii) affiche les mises en garde appropriées conformes aux dispositions sur la confidentialité s'il interdit les activités de surveillance, d'enregistrement ou de vérification et (iii) inclut dans l'avis aux utilisateurs publics du système une description de l'utilisation autorisée du système.	
AC-9	AVIS CONCERNANT LES CONNEXIONS ANTÉRIEURES (ACCÈS)	(A) Le système d'information indique à l'utilisateur qui a réussi à se connecter la date et l'heure de sa dernière connexion (dernier accès).	

Numéro	Nom	Définition	Affectation
AC-9.1	AVIS CONCERNANT LES CONNEXIONS ANTÉRIEURES (ACCÈS)	Le système indique à l'utilisateur qui a réussi à se connecter le nombre de tentatives de connexions infructueuses depuis sa dernière connexion réussie.	
AC-9.2	AVIS CONCERNANT LES CONNEXIONS ANTÉRIEURES (ACCÈS)	Le système indique à l'utilisateur le nombre de [Sélection : connexions/accès réussies; connexions/accès non réussies; les deux] pendant [Affectation : durée définie par l'organisation].	
AC-9.3	AVIS CONCERNANT LES CONNEXIONS ANTÉRIEURES (ACCÈS)	Le système informe l'utilisateur de [Affectation : ensemble de modifications, défini par l'organisation, liées à la sécurité et apportées au compte de l'utilisateur] pendant [Affectation : durée définie par l'organisation].	
AC-11	VERROUILLAGE DE SESSION	(A) Le système d'information empêche tout autre accès au système en verrouillant la session après [Affectation : durée définie par l'organisation] d'inactivité ou sur réception d'une demande d'un utilisateur. (B) Le système d'information maintient le verrouillage de la session jusqu'à ce que l'utilisateur réinitialise l'accès en exécutant les procédures établies d'identification et d'authentification.	(A) Période de temps [après une période ne dépassant pas 60 minutes]
AC-11.1	VERROUILLAGE DE SESSION	Le mécanisme de verrouillage de session du système d'information, lorsqu'il est activé dans un dispositif doté d'un écran, affiche différents motifs visibles qui permettent de cacher ce qui figurait précédemment à l'écran.	
AC-14	OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION	(A) L'organisation identifie les opérations spécifiques que l'utilisateur peut exécuter dans le système sans s'identifier ni s'authentifier. (B) L'organisation documente et explique dans le plan de sécurité des opérations du système la logique sous-jacente qui permet à l'utilisateur d'effectuer des opérations qui ne nécessitent ni identification ni authentification.	
AC-14.1	OPÉRATIONS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION	L'organisation permet d'effectuer des opérations sans contrôle d'identification ni d'authentification seulement dans la mesure où cela est nécessaire pour atteindre des objectifs opérationnels ou liés à la mission.	
AC-17	ACCÈS À DISTANCE	(A) L'organisation documente les méthodes autorisées d'accès à distance du système d'information. (B) L'organisation définit les restrictions d'utilisation et les directives de mise en œuvre de chaque méthode d'accès à distance autorisée. (C) L'organisation surveille les accès à distance non autorisés du système d'information. (D) L'organisation autorise l'accès à distance du système d'information avant la connexion. (E) L'organisation applique les exigences concernant les connexions à distance du système d'information. (AA) L'organisation s'assure que tous les employés qui travaillent à l'extérieur des locaux protègent l'information conformément aux exigences minimales de la Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7].	
AC-17.5	ACCÈS À DISTANCE	L'organisation surveille l'existence de connexions à distance non autorisées au système [Affectation : fréquence définie par l'organisation] et prend des mesures appropriées le cas échéant.	(5) Fréquence [en continu]

Numéro	Nom	Définition	Affectation
AC-18	ACCÈS SANS FIL	(A) L'organisation établit les restrictions d'utilisation et les directives de mise en œuvre de l'accès sans fil. (B) L'organisation surveille l'existence d'accès sans fil non autorisés au système d'information. (C) L'organisation autorise l'accès sans fil au système d'information avant la connexion. (D) L'organisation applique les exigences concernant les connexions sans fil au système d'information.	
AC-18.2	ACCÈS SANS FIL	L'organisation surveille la présence de connexions sans fil non autorisées au système d'information, incluant l'analyse des points d'accès sans fil non autorisés [Affectation : fréquence définie par l'organisation], et prend des mesures appropriées le cas échéant.	(2) Fréquence [en continu]
AC-18.3	ACCÈS SANS FIL	L'organisation désactive, lorsqu'elle ne prévoit pas les utiliser, les capacités de réseautage sans fil intégrées aux composantes de système avant leur déploiement.	
AC-18.4	ACCÈS SANS FIL	L'organisation ne permet pas aux utilisateurs de configurer eux-mêmes les capacités de réseautage sans fil.	
AC-19	CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES	(A) L'organisation établit les restrictions d'utilisation et donne des directives sur les dispositifs mobiles contrôlés par l'organisation. (B) L'organisation autorise la connexion des dispositifs mobiles qui répondent à ses restrictions d'utilisation et aux directives de mise en œuvre des systèmes d'information organisationnels. (C) L'organisation surveille les connexions non autorisées des dispositifs mobiles aux systèmes d'information organisationnels. (D) L'organisation applique les exigences concernant la connexion des dispositifs mobiles à ses systèmes d'information. (E) L'organisation désactive les fonctions du système d'information qui permettent l'exécution automatique du code des dispositifs mobiles sans l'autorisation de l'utilisateur. (F) L'organisation remet, en conformité avec ses politiques et procédures, des dispositifs mobiles spécialement configurés aux individus qui se déplacent dans des emplacements qui, selon elle, présentent des risques importants. (G) L'organisation applique [Affectation : mesures d'inspection et préventives définies par l'organisation], en conformité avec ses politiques et procédures, aux dispositifs mobiles à leur retour des emplacements qui, selon elle, présentent des risques importants.	
AC-19.1	CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES	L'organisation restreint l'utilisation des supports amovibles inscriptibles dans ses systèmes d'information.	
AC-19.2	CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES	L'organisation interdit l'utilisation des supports amovibles personnels dans ses systèmes d'information.	
AC-19.3	CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES	L'organisation interdit l'utilisation de supports amovibles dont le propriétaire est inconnu dans ses systèmes d'information.	

Numéro	Nom	Définition	Affectation
AC-19.100	CONTRÔLE D'ACCÈS AUX DISPOSITIFS MOBILES	L'organisation s'assure que les utilisateurs désactivent les dispositifs sans fil dotés d'une capacité de transmission de la voix, ou qu'ils en retirent manuellement le microphone lorsqu'ils participent à des réunions au cours desquelles il y a partage d'information classifiée, protégée B ou protégée C, conformément à la Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].	
AC-20	UTILISATION DES SYSTÈMES D'INFORMATION EXTERNES	(A) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent et (ou) maintiennent des systèmes d'information externes, définit les modalités selon lesquelles des individus, à partir de systèmes externes, sont autorisés à accéder au système d'information. (B) L'organisation, conformément aux relations de confiance établies avec d'autres organisations qui possèdent, exploitent et (ou) maintiennent des systèmes d'information externes, définit les modalités selon lesquelles des individus, à partir de systèmes externes, sont autorisés à traiter, stocker et (ou) transmettre de l'information qu'elle contrôle.	
AC-20.1	UTILISATION DES SYSTÈMES D'INFORMATION EXTERNES	L'organisation permet à des individus autorisés d'utiliser un système externe pour accéder à son système d'information ou pour traiter, stocker ou transmettre de l'information sous son contrôle seulement lorsqu'elle : (a) Peut s'assurer que le système externe applique les contrôles de sécurité requis tel que stipulé dans sa politique de sécurité de l'information et le plan de sécurité; ou (b) A approuvé les ententes de connexion ou de traitement avec l'entité organisationnelle qui héberge le système externe.	
AC-20.2	UTILISATION DES SYSTÈMES D'INFORMATION EXTERNES	L'organisation limite, dans les systèmes externes, l'utilisation par des individus autorisés des supports de stockage amovibles qu'elle contrôle.	
AC-21	COLLABORATION ET PARTAGE D'INFORMATION ENTRE UTILISATEURS	(A) L'organisation facilite le partage d'information en permettant aux utilisateurs autorisés de déterminer si les autorisations d'accès accordées aux partenaires de partage respectent les restrictions d'accès à l'information en tenant compte [Affectation : circonstances de partage d'information définies par l'organisation où l'utilisateur doit faire preuve de discrétion]. (B) L'organisation utilise [Affectation : liste définie par l'organisation des circonstances de partage d'information et des mécanismes automatisés ou des processus manuels requis] pour aider les utilisateurs à prendre des décisions concernant le partage d'information et la collaboration.	
AC-21.100	COLLABORATION ET PARTAGE D'INFORMATION ENTRE UTILISATEURS	L'organisation, suite à des ententes écrites, veille à prendre les mesures de protection appropriées de l'information sensible partagée avec d'autres gouvernements et organisations.	

Numéro	Nom	Définition	Affectation
AC-22	CONTENU ACCESSIBLE AU PUBLIC	(A) L'organisation désigne les individus autorisés à afficher de l'information dans les systèmes organisationnels accessibles au public. (B) L'organisation forme les individus autorisés afin de s'assurer que l'information accessible au public ne contienne aucune information sensible confidentielle. (C) L'organisation examine le contenu proposé de l'information mise à la disposition du public pour s'assurer qu'elle ne contienne aucune information sensible confidentielle avant qu'elle ne soit affichée dans le système organisationnel. (D) L'organisation examine [Affectation : fréquence définie par l'organisation] le contenu de l'information mise à la disposition du public pour s'assurer qu'elle ne contient aucune information sensible confidentielle]. (E) L'organisation, le cas échéant, retire toute information sensible confidentielle du système organisationnel accessible au public.	
AT-1	POLITIQUE ET PROCÉDURES DE FORMATION ET DE SENSIBILISATION À LA SÉCURITÉ	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de formation et de sensibilisation à la sécurité formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité. (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de formation et de sensibilisation à la sécurité et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
AT-2	SENSIBILISATION À LA SÉCURITÉ	(A) L'organisation dispense une formation de base de sensibilisation à la sécurité à tous les utilisateurs du système d'information (incluant les gestionnaires, les cadres supérieurs et les entrepreneurs) dans le cadre de la formation initiale des nouveaux utilisateurs; la formation est offerte lorsque les changements apportés au système le justifient, et à tous les [Affectation : fréquence définie par l'organisation] par la suite.	
AT-3	FORMATION À LA SÉCURITÉ	(A) L'organisation offre une formation à la sécurité axée sur les rôles (i) avant d'autoriser l'accès au système ou l'exécution des tâches reliées au poste de l'utilisateur, (ii) lorsque les modifications apportées au système l'exigent et (iii) [Affectation : fréquence définie par l'organisation] par la suite.	
AT-4	DOSSIERS DE FORMATION À LA SÉCURITÉ	(A) L'organisation documente et surveille les activités individuelles de formation à la sécurité des systèmes d'information, incluant la formation de sensibilisation de base et la formation spécifique à la sécurité des systèmes d'information. (B) L'organisation conserve les dossiers de formation individuels pendant [Affectation : durée définie par l'organisation].	

Numéro	Nom	Définition	Affectation
AU-1	POLITIQUE ET PROCÉDURES DE VÉRIFICATION ET DE RESPONSABILISATION	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de vérification et de responsabilisation formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité. (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de vérification et de responsabilisation et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
AU-2	ÉVÉNEMENTS VÉRIFIABLES	(A) L'organisation détermine, à partir d'une évaluation des risques et des besoins opérationnels et de la mission, la capacité du système d'information de vérifier les événements suivants : [Affectation : liste des événements vérifiables définie par l'organisation]. (B) L'organisation coordonne la fonction de vérification de la sécurité avec d'autres entités organisationnelles ayant les mêmes besoins pour favoriser le soutien mutuel et faciliter la sélection des événements vérifiables. (C) L'organisation explique pourquoi la liste des événements vérifiables est jugée adéquate pour soutenir les enquêtes après le fait des incidents de sécurité. (D) L'organisation détermine, à partir de l'information actuelle sur les menaces et de l'évaluation continue des risques, si les événements suivants doivent être vérifiés dans le système d'information : [Affectation : sous-ensemble défini par l'organisation des événements vérifiables définis en AU-2 a. qui doivent être vérifiés, incluant la fréquence de vérification (ou la situation qui justifie la vérification) de chacun].	(A) Liste d'événements [ports de la console de gestion et des opérations et ports de communication accessibles publiquement]
AU-2.3	ÉVÉNEMENTS VÉRIFIABLES	L'organisation examine et met à jour la liste des événements vérifiables [Affectation : fréquence définie par l'organisation].	(3) Fréquence [à une fréquence ne dépassant par une fois l'an]
AU-2.4	ÉVÉNEMENTS VÉRIFIABLES	L'organisation inclut l'exécution de fonctions privilégiées dans la liste des événements à vérifier par le système.	
AU-3	CONTENU DES DOSSIERS DE VÉRIFICATION	(A) Le système d'information produit des dossiers de vérification qui contiennent suffisamment d'information pour permettre, au minimum, d'établir le type d'événement qui s'est produit, la date et l'heure de l'événement, l'endroit où il s'est produit, sa source, son résultat (réussite ou échec) et l'identité de tous les utilisateurs ou sujets qui lui sont associés.	
AU-3.1	CONTENU DES DOSSIERS DE VÉRIFICATION	Le système inclut [Affectation : information supplémentaire et plus détaillée définie par l'organisation], répartie par type, emplacement ou sujet, dans les dossiers de vérification des événements.	
AU-3.2	CONTENU DES DOSSIERS DE VÉRIFICATION	L'organisation centralise la gestion du contenu des dossiers de vérification produits par [Affectation : composantes de système définies par l'organisation].	(2) Hôtes de la GJI avec sauvegarde centrale
AU-5	INTERVENTION EN CAS DE PROBLÈMES DE TRAITEMENT	(A) Le système d'information avertit les agents désignés de l'organisation dans l'éventualité d'un problème de traitement des vérifications. (B) Le système d'information prend les mesures supplémentaires suivantes : [Affectation : mesures à prendre définies par l'organisation (p. ex., arrêt du système, écrasement des vieux fichiers de vérification, arrêt de production de fichiers de vérification)].	(B) Mesure [écrasement]

Numéro	Nom	Définition	Affectation
AU-5.1	INTERVENTION EN CAS DE PROBLÈMES DE TRAITEMENT	Le système produit un avertissement lorsque le volume attribué de stockage des dossiers de vérification atteint [Affectation : pourcentage défini par l'organisation] de la capacité maximale.	(1) Pourcentage [75 %]
AU-6	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	(A) L'organisation examine et analyse les dossiers de vérification du système d'information [Affectation : fréquence définie par l'organisation] pour déceler toute activité inappropriée ou inhabituelle et remet ses constatations à ses agents désignés. (B) L'organisation ajuste le niveau d'examen, d'analyse et de rapports de vérification du système d'information lorsqu'il y a une variation du risque pour les activités et les biens organisationnels, les individus, les autres organisations ou le Canada suite à la réception de renseignements et d'information concernant le respect des lois, ou d'information en provenance d'autres sources crédibles.	
AU-6.1	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	Le système intègre les processus d'examen, d'analyse et de rapports des vérifications pour soutenir les processus organisationnels d'enquête et d'intervention en cas d'activités suspectes.	
AU-6.3	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	L'organisation analyse et met en corrélation les dossiers de vérification des différents dépôts afin de se sensibiliser à sa situation globale.	
AU-6.4	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	Le système centralise l'examen et l'analyse des dossiers de vérification de plusieurs composantes du système.	
AU-6.7	EXAMEN, ANALYSE ET RAPPORTS DE VÉRIFICATION	L'organisation précise, dans la politique de vérification et de responsabilisation, les mesures autorisées pour chaque processus de système, rôle et (ou) utilisateur approuvé.	
AU-7	RÉDUCTION DES VÉRIFICATIONS ET PRODUCTION DES RAPPORTS	(A) Le système d'information offre une capacité de réduction des vérifications et de production des rapports.	
AU-7.1	RÉDUCTION DES VÉRIFICATIONS ET PRODUCTION DES RAPPORTS	Le système permet, à partir de critères d'événement sélectionnables, de traiter automatiquement les dossiers de vérification des événements d'intérêt.	
AU-8	TIMBRES HORODATEURS	(A) Le système d'information utilise des horloges de système internes pour produire des timbres horodateurs pour les dossiers de vérification.	
AU-8.1	TIMBRES HORODATEURS	Le système synchronise les horloges internes [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : source horaire autorisée définie par l'organisation].	(1) Fréquence [période ne dépassant pas un jour] (1) Temps [source horaire définie par un autorisateur]
AU-9	PROTECTION DE L'INFORMATION DE VÉRIFICATION	(A) Le système d'information protège l'information de vérification et les outils de vérification contre tout accès, modification et suppression non autorisés.	
AU-9.2	PROTECTION DE L'INFORMATION DE VÉRIFICATION	Le système effectue une sauvegarde des dossiers de vérification [Affectation : fréquence définie par l'organisation] dans un système ou des supports différents du système qui fait l'objet de la vérification.	

Numéro	Nom	Définition	Affectation
AU-9.4	PROTECTION DE L'INFORMATION DE VÉRIFICATION	L'organisation : (a) Accorde l'accès à la fonction de gestion de la vérification uniquement à un nombre restreint d'utilisateurs privilégiés; et (b) Protège les dossiers de vérification des accès distants aux comptes privilégiés et des exécutions de fonctions privilégiées.	
AU-10	NON-RÉPUDIATION	(A) Le système d'information offre une protection contre quiconque nie faussement avoir effectué une opération particulière.	
AU-10.5	NON-RÉPUDIATION	L'organisation utilise un mécanisme cryptographique conforme aux exigences du contrôle SC-13 concernant l'application des signatures numériques.	
AU-11	CONSERVATION DES DOSSIERS DE VÉRIFICATION	(A) L'organisation conserve les dossiers de vérification pendant [Affectation : durée définie par l'organisation et conforme à la politique de conservation des dossiers] pour soutenir les enquêtes après le fait effectuées sur les incidents de sécurité et satisfaire aux exigences règlementaires et organisationnelles de conservation de l'information.	Tel que l'exige la loi.
AU-12	PRODUCTION DES DOSSIERS DE VÉRIFICATION	(A) Le système d'information inclut une capacité de production de dossiers de vérification pour les événements vérifiables définis dans la liste de [Affectation : composantes de système définies par l'organisation] du contrôle AU-2]. (B) Le système d'information permet au personnel désigné de l'organisation de sélectionner, par composante de système particulière, les événements vérifiables qui doivent être vérifiés. (C) Le système d'information produit des dossiers de vérification pour les événements vérifiables définis dans la liste du contrôle AU-2 et dont le contenu est défini au contrôle AU-3.	(A) Composantes [composantes définies par l'autorisateur]
AU-12.1	PRODUCTION DES DOSSIERS DE VÉRIFICATION	Le système compile les dossiers de vérification des [Affectation : composantes de système définies par l'organisation] en une piste de vérification (logique ou physique) globale et établit une corrélation chronologique [Affectation : niveau de tolérance défini par l'organisation des relations entre les timbres horodateurs des dossiers individuels de la piste de vérification].	
AU-12.2	PRODUCTION DES DOSSIERS DE VÉRIFICATION	Le système produit une piste de vérification (logique ou physique) globale composée de dossiers de vérification dont le format est normalisé.	
CA-1	POLITIQUE ET PROCÉDURES D'ÉVALUATION ET D'AUTORISATION DE LA SÉCURITÉ	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des politiques d'évaluation et d'autorisation de la sécurité formelles et documentées qui définissent les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité. (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'évaluation et d'autorisation de la sécurité et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]

Numéro	Nom	Définition	Affectation
CA-2	ÉVALUATIONS DE LA SÉCURITÉ	(A) L'organisation développe un plan d'évaluation de la sécurité qui décrit la portée de l'évaluation, incluant ce qui suit : (a) Contrôles de sécurité et améliorations de contrôle sous évaluation; (b) Procédures d'évaluation servant à déterminer l'efficacité des contrôles de sécurité; et (c) Environnement d'évaluation, équipe d'évaluation et rôles et responsabilités liés à l'évaluation. (B) L'organisation évalue les contrôles de sécurité du système d'information [Affectation : fréquence définie par l'organisation] pour déterminer la mesure dans laquelle ils sont appliqués correctement, fonctionnent tel que prévu et produisent les résultats souhaités dans le respect des exigences relatives au contrôle de sécurité des systèmes. (C) L'organisation produit un rapport d'évaluation de la sécurité qui documente les résultats de l'évaluation. (D) L'organisation remet, par écrit, les résultats de l'évaluation à l'agent d'autorisation ou à un représentant désigné.	(B) Fréquence [Fréquence déterminée par l'autorisateur]
CA-2.2	ÉVALUATIONS DE LA SÉCURITÉ	L'organisation intègre aux évaluations des contrôles de sécurité, [Affectation : fréquence définie par l'organisation], [Sélection : avec préavis, sans préavis], [Sélection : surveillance en profondeur; test de détection d'utilisateur malveillant; test de pénétration; exercices de l'équipe d'intervention; [Affectation : autres formes de test de sécurité définies par l'organisation]].	
CA-3	CONNEXIONS DES SYSTÈMES D'INFORMATION	(A) L'organisation autorise les connexions du système d'information à d'autres systèmes sur lesquels elle n'a aucune autorité en recourant à des ententes sur la sécurité des interconnexions. (B) L'organisation documente, pour chaque connexion, les caractéristiques d'interface, les exigences des contrôles de sécurité et la nature de l'information communiquée. (C) L'organisation surveille en permanence les connexions du système d'information et vérifie le respect des exigences en matière de contrôle de sécurité.	
CA-5	PLAN DE MISE EN OEUVRE DES MESURES DE PROTECTION (PLAN D'ACTION ET JALONS)	(A) L'organisation développe un plan d'action et des jalons pour le système d'information afin de documenter les mesures correctives qu'elle prévoit utiliser pour corriger les faiblesses ou les lacunes relevées durant l'évaluation des contrôles de sécurité et pour réduire et éliminer les vulnérabilités connues du système. (B) L'organisation met à jour le plan d'action et les jalons existants [Affectation : fréquence définie par l'organisation] en tenant compte des constatations des évaluations de contrôles de sécurité, des analyses des répercussions sur la sécurité et des activités de surveillance permanente.	(B) Fréquence [Fréquence déterminée par l'autorisateur]
CA-6	AUTORISATION DE SÉCURITÉ	(A) L'organisation attribue à un cadre supérieur ou à un gestionnaire le rôle d'agent d'autorisation du système d'information. (B) L'organisation s'assure que l'agent autorise le système d'information aux fins de traitement avant d'en commencer l'exploitation. (C) L'organisation met à jour l'autorisation de sécurité [Affectation : fréquence définie par l'organisation].	(C) Fréquence [Fréquence déterminée par l'autorisateur]

Numéro	Nom	Définition	Affectation
CA-7	SURVEILLANCE PERMANENTE	(A) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut un processus de gestion de la configuration du système d'information et de ses composantes. (B) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut une détermination, sur le plan de la sécurité, de l'incidence des modifications apportées au système d'information et à l'environnement d'exploitation. (C) L'organisation développe une stratégie de surveillance permanente et met en œuvre un programme de surveillance permanente qui inclut des évaluations permanentes des contrôles de sécurité, en conformité avec sa stratégie de surveillance permanente. (D) L'organisation développe une stratégie de surveillance permanente et met en oeuvre un programme de surveillance permanente qui inclut la déclaration de l'état de sécurité du système d'information aux agents concernés de l'organisation [Affectation : fréquence définie par l'organisation].	
CA-7.2	SURVEILLANCE PERMANENTE	L'organisation prévoit, planifie et effectue les évaluations [Affectation : fréquence définie par l'organisation], [Sélection : avec préavis, sans préavis], [Sélection : surveillance en profondeur; test de détection d'utilisateur malveillant; test de pénétration; exercices de l'équipe d'intervention; [Affectation : autres formes de test de sécurité définies par l'organisation]] pour assurer la conformité à toutes les procédures d'atténuation des vulnérabilités.	
CM-1	POLITIQUE ET PROCÉDURES DE GESTION DE LA CONFIGURATION	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de gestion de la configuration formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité. (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de gestion de la configuration et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
CM-2	CONFIGURATION DE BASE	(A) L'organisation développe, documente et tient à jour la configuration de base actuelle du système d'information.	
CM-2.1	CONFIGURATION DE BASE	L'organisation examine et met à jour la configuration de base du système d'information : (a) [Affectation : fréquence définie par l'organisation]; (b) Le cas échéant, [Affectation : circonstances définies par l'organisation]; et (c) Dans le cadre des installations et des mises à niveau des composantes du système d'information.	
CM-2.2	CONFIGURATION DE BASE	L'organisation utilise des mécanismes automatisés pour assurer le maintien d'une configuration de base à jour, complète, précise et facilement accessible.	

Numéro	Nom	Définition	Affectation
CM-2.5	CONFIGURATION DE BASE	L'organisation : (a) Développe et maintient [Affectation : liste définie par l'organisation des programmes qui peuvent être exécutés dans le système]; et (b) Utilise une politique d'autorisation (tout interdire, permettre par exception) pour identifier le logiciel qui peut être exécuté dans le système d'information.	
CM-2.6	CONFIGURATION DE BASE	L'organisation maintient pour les environnements de développement et de test une configuration de base gérée séparément de la configuration opérationnelle.	
CM-3	CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION	(A) L'organisation détermine les types de modification du système d'information qui sont liés à la configuration. (B) L'organisation approuve les modifications liées à la configuration en tenant compte explicitement des analyses des répercussions sur la sécurité. (C) L'organisation documente les modifications approuvées liées à la configuration. (D) L'organisation conserve et examine les dossiers des modifications liées à la configuration. (E) L'organisation vérifie les activités relatives aux modifications liées à la configuration. (F) L'organisation coordonne et surveille les activités de contrôle des modifications de la configuration par [Affectation : élément de contrôle des modifications de la configuration défini par l'organisation (p. ex., comité, conseil) qui se réunit [Sélection : (une ou plusieurs) : [Affectation : fréquence définie par l'organisation]]; [Affectation : conditions de modification de la configuration définies par l'organisation].	(F) [Conseil de gestion de la configuration]
CM-3.1	CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION	L'organisation utilise des mécanismes automatisés pour : (a) Documenter les modifications proposées au système d'information; (b) Informer les autorités d'approbation désignées; (c) Souligner les approbations qui n'ont pas été reçues le ou avant le [Affectation : durée définie par l'organisation]; (d) Retenir les modifications jusqu'à la réception des approbations des autorités désignées; et (e) Documenter les modifications qui ont été effectuées.	
CM-3.2	CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION	L'organisation teste, valide et documente les modifications avant de les inclure dans le système opérationnel.	
CM-3.3	CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION	L'organisation utilise des mécanismes automatisés pour apporter les modifications au système de base actuel et les déploie ensuite dans l'ensemble des systèmes installés.	
CM-3.4	CONTRÔLE DES MODIFICATIONS DE LA CONFIGURATION	L'organisation exige qu'un représentant de la sécurité de l'information soit membre de [Affectation : élément de contrôle des modifications de la configuration (p. ex., comité, conseil) défini par l'organisation].	
CM-4	ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ	(A) L'organisation analyse, avant de les mettre en œuvre, les modifications apportées au système d'information pour déterminer leurs éventuelles répercussions sur la sécurité.	
CM-4.1	ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ	L'organisation analyse les nouveaux logiciels dans un environnement de test distinct avant de les installer dans un environnement opérationnel afin de déceler toute lacune, faiblesse, incompatibilité ou intention malveillante susceptible d'influer sur la sécurité.	

Numéro	Nom	Définition	Affectation
CM-4.2	ANALYSE DES RÉPERCUSSIONS SUR LA SÉCURITÉ	L'organisation, après que les modifications ont été apportées au système, vérifie les fonctions de sécurité pour s'assurer qu'elles ont été mises en œuvre correctement, qu'elles fonctionnent tel que prévu et qu'elles produisent les résultats souhaités, conformément aux exigences du contrôle de la sécurité des systèmes.	
CM-5	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	(A) L'organisation définit, documente, approuve et applique les restrictions d'accès logique et physique associées aux modifications du système d'information.	
CM-5.1	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	L'organisation utilise des mécanismes automatisés pour appliquer les restrictions d'accès et faciliter la vérification des mesures d'application.	
CM-5.2	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	L'organisation vérifie les modifications apportées au système d'information [Affectation : fréquence définie par l'organisation] et, le cas échéant, détermine s'il y a eu des modifications non autorisées.	(2) [Au moins une fois tous les 12 mois]
CM-5.4	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	L'organisation applique la règle des deux personnes pour les modifications de [Affectation : information système et composantes de système définies par l'organisation].	(4) [Liste fournie par l'autorisateur]
CM-5.5	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	L'organisation : (a) Restreint les privilèges accordés aux développeurs et (ou) aux intégrateurs de système pour ce qui touche les modifications, directement dans l'environnement de production, des composantes matérielles, logicielles et micrologicielles et du système d'information; et (b) Examine et réévalue les privilèges accordés aux développeurs et (ou) aux intégrateurs de système [Affectation : fréquence définie par l'organisation].	
CM-5.6	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	L'organisation restreint les privilèges de modification du logiciel inclus dans les bibliothèques de logiciel (incluant les programmes privilégiés).	
CM-5.7	RESTRICTIONS D'ACCÈS ASSOCIÉES AUX MODIFICATIONS	Le système applique automatiquement [Affectation : mesures de protection et contremesures définies par l'organisation] lorsque les fonctions (ou mécanismes) de sécurité sont modifiées de manière inappropriée.	
CM-6	PARAMÈTRES DE CONFIGURATION	(A) L'organisation établit et documente les paramètres obligatoires de configuration des produits de technologie de l'information intégrés au système d'information en utilisant des [Affectation : listes de vérification de la sécurité de la configuration définies par l'organisation] qui incluent les restrictions les plus strictes stipulées dans les exigences opérationnelles. (B) L'organisation applique les paramètres de configuration. (C) L'organisation identifie, documente et approuve les exceptions aux paramètres obligatoires de configuration des composantes individuelles en tenant compte d'exigences opérationnelles explicites. (D) L'organisation surveille et contrôle les modifications des paramètres de configuration en conformité avec ses politiques et procédures.	(A) [Liste de vérification approuvée par un autorisateur]
CM-6.1	PARAMÈTRES DE CONFIGURATION	L'organisation utilise des mécanismes automatisés pour centraliser la gestion, l'application et la vérification des paramètres de configuration.	
CM-6.2	PARAMÈTRES DE CONFIGURATION	L'organisation utilise des mécanismes automatisés pour intervenir en cas de modification non autorisée des [Affectation : paramètres définis par l'organisation de configuration].	

Numéro	Nom	Définition	Affectation
CM-6.3	PARAMÈTRES DE CONFIGURATION	L'organisation intègre un mécanisme de détection des modifications non autorisées de la configuration à sa capacité d'intervention en cas d'incident pour s'assurer de pister, surveiller, corriger et conserver à des fins historiques les événements concernés.	
CM-6.4	PARAMÈTRES DE CONFIGURATION	Le système (et les modifications apportées à la configuration de base) doit démontrer qu'il se conforme aux directives de configuration de la sécurité (c.-à-d., les listes de vérification de la sécurité) avant d'être déployé dans l'environnement de production.	
CM-7	FONCTIONNALITÉ MINIMALE	(A) L'organisation configure le système d'information de manière à offrir uniquement les capacités jugées essentielles et interdit ou restreint spécifiquement l'utilisation des fonctions, ports, protocoles et (ou) services suivants : [Affectation : liste définie par l'organisation des fonctions, ports, protocoles et (ou) services interdits ou restreints].	(1) [Liste des fonctions, ports, protocoles et (ou) services interdits ou restreints]
CM-7.1	FONCTIONNALITÉ MINIMALE	L'organisation examine le système d'information [Affectation : fréquence définie par l'organisation] pour identifier et supprimer les fonctions, ports, protocoles et (ou) services non requis.	(1) Fréquence [à une fréquence ne dépassant par une fois l'an]
CM-7.3	FONCTIONNALITÉ MINIMALE	L'organisation assure le respect des [Affectation : exigences d'enregistrement définies par l'organisation concernant les ports, protocoles et services].	
CM-8	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	(A) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information qui reflète correctement le système d'information actuel. (B) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information conforme à la limite d'autorisation du système d'information. (C) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information au niveau de granularité jugé nécessaire pour permettre le suivi et la production de rapports. (D) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information qui inclut [Affectation : information définie par l'organisation et jugée nécessaire à la réalisation d'une comptabilisation efficace des immobilisations]. (E) L'organisation développe, documente et tient à jour un inventaire des composantes de système d'information que les agents désignés de l'organisation peuvent examiner et vérifier.	
CM-8.1	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation met à jour l'inventaire des composantes de système d'information dans le cadre des activités d'installation et de retrait des composantes et de mise à jour du système.	
CM-8.2	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation utilise des mécanismes automatisés pour faciliter la tenue à jour d'un inventaire de composantes à jour, complet, précis et facilement accessible.	
CM-8.3	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation : (a) Utilise des mécanismes automatisés [Affectation : fréquence définie par l'organisation] pour détecter l'ajout de toute composante et (ou) de tout dispositif non autorisés au système d'information; et (b) Désactive l'accès réseau de ces composantes et (ou) dispositifs ou informe les agents désignés de l'organisation.	

Numéro	Nom	Définition	Affectation
CM-8.4	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation inclut, dans les données sur la comptabilité des biens, de l'information sur les composantes de système comme moyen d'identifier par [Sélection (une valeur ou plus) : nom; poste; rôle] les individus responsables de l'administration de ces composantes.	
CM-8.5	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation vérifie que toutes les composantes incluses dans la limite d'autorisation du système soit figurent dans l'inventaire du système, soit sont reconnues par autre système comme composante du système.	
CM-8.6	INVENTAIRE DES COMPOSANTES DE SYSTÈME D'INFORMATION	L'organisation inclut dans l'inventaire des composantes les configurations de composantes évaluées et les déviations approuvées pour les configurations déjà déployées.	
CM-9	PLAN DE GESTION DE LA CONFIGURATION	(A) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui traite des rôles, des responsabilités et des processus et procédures de gestion de la configuration. (B) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui définit les éléments de configuration du système et précise à quel moment les éléments sont gérés dans le cycle de développement des systèmes. (C) L'organisation développe, documente et met en œuvre pour le système d'information un plan de gestion de la configuration qui définit les moyens d'identifier les éléments de configuration durant le cycle de développement des systèmes ainsi qu'un processus de gestion de leur configuration.	
CP-1	POLITIQUE ET PROCÉDURES DE PLANIFICATION D'URGENCE	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de planification d'urgence formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de planification d'urgence et des contrôles correspondants. (AA L'organisation développe un cycle de vérification du programme de planification d'urgence comme base de déclaration régulière au SCT.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]

Numéro	Nom	Définition	Affectation
CP-2	PLAN DES MESURES D'URGENCE	(A) L'organisation développe pour le système d'information un plan de mesures d'urgence qui : (a) Identifie les fonctions opérationnelles et de mission essentielles et les exigences d'urgence connexes; (b) Définit les objectifs de reprise, les priorités de restauration et les paramètres; (c) Identifie les rôles et responsabilités liés aux urgences et les individus assignés à ces fonctions, incluant l'information pour les contacter; (d) Souligne le besoin de maintenir les fonctions opérationnelles et de mission essentielles en dépit de toute perturbation, compromission ou défaillance du système d'information; (e) Traite de la restauration complète du système d'information sans détérioration des mesures de sécurité initialement prévues et instaurées; et (f) Est révisé et approuvé par des agents désignés de l'organisation. (B) L'organisation distribue des copies du plan des mesures d'urgence à [Affectation : liste (par nom et (ou) rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels]. (C) L'organisation coordonne les activités de planification d'urgence avec les activités de traitement des incidents. (D) L'organisation examine le plan des mesures d'urgence du système d'information [Affectation : fréquence définie par l'organisation]. (E) L'organisation révise le plan des mesures d'urgence pour tenir compte des changements apportés à l'organisation, au système d'information ou à l'environnement d'exploitation et des problèmes rencontrés lors de la mise en œuvre, de l'exécution ou des tests du plan. (F) L'organisation communique les modifications du plan des mesures d'urgence à [Affectation : liste (par nom et (ou) rôle) définie par l'organisation des principaux responsables des mesures d'urgence et des éléments organisationnels].	(D) [à une fréquence ne dépassant par une fois l'an]
CP-2.1	PLAN DES MESURES D'URGENCE	L'organisation coordonne le développement du plan des mesures d'urgence avec les éléments organisationnels responsables des plans connexes.	
CP-2.2	PLAN DES MESURES D'URGENCE	L'organisation planifie la capacité de manière à disposer des ressources nécessaires pour traiter l'information, utiliser les télécommunications et soutenir l'environnement durant les opérations d'urgence.	
CP-2.3	PLAN DES MESURES D'URGENCE	L'organisation planifie la reprise des fonctions opérationnelles et de mission essentielles dans les [Affectation : durée définie par l'organisation] pour l'activation du plan des mesures d'urgence.	(3) [Dans les 24 heures]
CP-2.4	PLAN DES MESURES D'URGENCE	L'organisation planifie la reprise complète des fonctions opérationnelles et de mission dans les [Affectation : durée définie par l'organisation] pour l'activation du plan des mesures d'urgence.	

Numéro	Nom	Définition	Affectation
CP-2.5	PLAN DES MESURES D'URGENCE	L'organisation planifie la continuité des fonctions opérationnelles et de mission essentielles avec peu ou pas de perte au plan de la continuité des activités et maintient cet état jusqu'à la restauration complète du système d'information dans les sites principaux de traitement et (ou) de stockage.	
CP-2.6	PLAN DES MESURES D'URGENCE	L'organisation prévoit le transfert de toutes les fonctions opérationnelles et de mission essentielles vers des sites principaux de traitement et (ou) de stockage de secours avec peu ou pas de perte au plan de la continuité des activités, et maintient cet état pendant la restauration complète dans ces sites.	
CP-3	FORMATION SUR LES SITUATIONS D'URGENCE	(A) L'organisation assure la formation du personnel sur ses rôles et responsabilités lors des urgences liées au système d'information et offre des cours de recyclage [Affectation : fréquence définie par l'organisation].	
CP-4	TESTS ET EXERCICES RELATIFS AU PLAN DES MESURES D'URGENCE	(A) L'organisation teste et (ou) vérifie l'applicabilité du plan des mesures d'urgence du système d'information [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : tests et (ou) exercices définis par l'organisation] pour en déterminer l'efficacité et établir la mesure dans laquelle elle est prête à l'exécuter. (B) L'organisation examine les résultats des tests et des exercices relatifs au plan et entreprend des mesures correctrices.	(A) Fréquence [à une fréquence ne dépassant par une fois l'an]
CP-4.1	TESTS ET EXERCICES RELATIFS AU PLAN DES MESURES D'URGENCE	L'organisation coordonne les tests et (ou) les exercices relatifs au plan des mesures d'urgence avec les éléments organisationnels responsables des plans connexes.	
CP-4.2	TESTS ET EXERCICES RELATIFS AU PLAN DES MESURES D'URGENCE	L'organisation teste et (ou) vérifie l'applicabilité du plan des mesures d'urgence dans le site de traitement de secours afin de permettre au personnel de se familiariser avec l'installation et les ressources disponibles et d'évaluer la capacité du site de prendre en charge les opérations d'urgence.	
CP-6	SITES DE STOCKAGE DE SECOURS	(A) L'organisation établit un site de stockage de secours, incluant les ententes nécessaires pour permettre le stockage et la récupération de l'information sur la sauvegarde des systèmes.	
CP-6.1	SITES DE STOCKAGE DE SECOURS	L'organisation identifie un site de stockage de secours distinct du site principal afin de n'être pas assujettie aux mêmes risques.	
CP-6.2	SITES DE STOCKAGE DE SECOURS	L'organisation configure le site de secours de manière à faciliter les opérations de reprise en conformité avec les objectifs de temps et de point de reprise.	
CP-7	SITE DE TRAITEMENT DE SECOURS	(A) L'organisation établit un site de traitement de secours, incluant les ententes nécessaires pour permettre la reprise des opérations du système d'information pour les fonctions opérationnelles et de mission essentielles dans les [Affectation : durée conforme aux objectifs de temps de reprise définie par l'organisation], lorsque les capacités de traitement principales ne sont pas disponibles. (B) L'organisation s'assure que l'équipement et les fournitures nécessaires à la reprise des opérations sont disponibles dans le site de secours, ou qu'il existe des contrats pour qu'ils soient livrés à temps afin de respecter la durée de la reprise qu'elle a définie.	(A) [Ne dépassant pas 24 heures]

Numéro	Nom	Définition	Affectation
CP-7.1	SITE DE TRAITEMENT DE SECOURS	L'organisation identifie un site de traitement de secours distinct du site principal afin de n'être pas assujettie aux mêmes risques.	
CP-7.4	SITE DE TRAITEMENT DE SECOURS	L'organisation configure le site de traitement de secours de manière qu'il soit prêt à être utilisé comme site opérationnel pour le traitement des fonctions opérationnelles et de mission essentielles.	
CP-7.5	SITE DE TRAITEMENT DE SECOURS	L'organisation s'assure que le site de traitement de secours offre des mesures de protection de la sécurité de l'information équivalentes à celles du site principal.	
CP-9	SAUVEGARDE DES SYSTÈMES D'INFORMATION	(A) L'organisation effectue des sauvegardes des données d'utilisateur contenues dans le système d'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]. (B) L'organisation effectue des sauvegardes des données système contenues dans le système d'information [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]. (C) L'organisation effectue des sauvegardes de la documentation du système, incluant la documentation sur la sécurité, [Affectation : fréquence définie par l'organisation et conforme aux objectifs de temps et de point de reprise]. (D) L'organisation protège la confidentialité et l'intégrité de l'information sauvegardée dans le lieu de stockage, en conformité avec la Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7]. (AA) L'organisation détermine les périodes de conservation de l'information opérationnelle essentielle et des sauvegardes archivées.	(A) Fréquence [à une fréquence ne dépassant par une fois par jour]
CP-9.1	SAUVEGARDE DES SYSTÈMES D'INFORMATION	L'organisation effectue des tests de l'information de sauvegarde [Affectation : fréquence définie par l'organisation] pour vérifier la fiabilité des supports et l'intégrité de l'information.	(1) [au moins une fois par mois]
CP-9.2	SAUVEGARDE DES SYSTÈMES D'INFORMATION	L'organisation utilise un échantillon de l'information de sauvegarde pour restaurer certaines fonctions du système d'information dans le cadre des tests du plan des mesures d'urgence.	
CP-9.3	SAUVEGARDE DES SYSTÈMES D'INFORMATION	L'organisation conserve des copies de sauvegarde du système d'exploitation et des autres logiciels critiques du système d'information, ainsi que des copies de l'inventaire du système d'information (incluant les composantes matérielles, logicielles et micrologicielles), dans une installation distincte ou un conteneur résistant au feu situé hors de l'emplacement du système de production.	
CP-9.5	SAUVEGARDE DES SYSTÈMES D'INFORMATION	L'organisation transfère l'information sur la sauvegarde des systèmes d'information dans un site de stockage de secours [Affectation : durée et taux de transfert définis par l'organisation et conformes aux objectifs de temps et de point de reprise].	
CP-10	RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION	(A) L'organisation permet la récupération et la reconstitution du système d'information à un état connu après une interruption, une compromission ou une défaillance.	
CP-10.3	RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION	L'organisation prévoit des contrôles de sécurité compensatoires pour [Affectation : circonstances définies par l'organisation qui peuvent nuire à la récupération et à la reconstitution à un état connu].	

Numéro	Nom	Définition	Affectation
CP-10.4	RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION	L'organisation permet de rétablir l'image des composantes de système d'information dans les [Affectation : durées de restauration définies par l'organisation] en utilisant des images disque (dont la configuration est contrôlée et l'intégrité, protégée) représentant les composantes dans un état protégé et opérationnel.	
CP-10.5	RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION	L'organisation offre [Sélection : temps réel; temps presque réel] [Affectation : capacité de reprise définie par l'organisation].	
CP-10.6	RÉCUPÉRATION ET RECONSTITUTION DES SYSTÈMES D'INFORMATION	L'organisation protège le matériel, le micrologiciel et le logiciel de sauvegarde et de restauration.	
IA-1	POLITIQUE ET PROCÉDURES D'IDENTIFICATION ET D'AUTHENTIFICATION	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique d'identification et d'authentification formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'identification et d'authentification et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
IA-2	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	(A) Le système d'information identifie de façon unique et authentifie les utilisateurs organisationnels (ou les processus exécutés en leur nom).	
IA-2.1	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Le système utilise l'authentification multifactorielle pour l'accès réseau aux comptes privilégiés.	
IA-2.8	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Le système utilise [Affectation : mécanismes d'authentification résistants aux réinsertions définis par l'organisation] pour l'accès réseau aux comptes privilégiés.	Réinsertion [Mécanismes de réinsertion définis par l'autorisateur]
IA-2.9	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS)	Le système utilise [Affectation : mécanismes d'authentification résistants aux réinsertions définis par l'organisation] pour l'accès réseau aux comptes non privilégiés.	
IA-3	IDENTIFICATION ET AUTHENTIFICATION DES DISPOSITIFS	(A) Le système d'information identifie de façon unique et authentifie [Affectation : liste définie de dispositifs spécifiques et (ou) de types de dispositif] avant l'établissement d'une connexion.	
IA-4	GESTION DES IDENTIFICATEURS	(A) L'organisation gère les identificateurs d'utilisateur et de dispositif sous l'autorité d'un agent désigné de l'organisation chargé de leur attribution. (B) L'organisation gère les identificateurs d'utilisateur et de dispositif en sélectionnant un identificateur d'utilisateur ou de dispositif unique. (C) L'organisation gère les identificateurs d'utilisateur et de dispositif en attribuant l'identificateur à l'utilisateur ou au dispositif concerné. (D) L'organisation gère les identificateurs d'utilisateur et de dispositif en empêchant leur réutilisation pendant [Affectation : durée définie par l'organisation]. (E) L'organisation gère les identificateurs d'utilisateur et de dispositif en désactivant l'identificateur d'utilisateur après [Affectation : durée d'inactivité définie par l'organisation].	
IA-4.3	GESTION DES IDENTIFICATEURS	L'organisation exige plusieurs formes de certification d'identification individuelle, telle la présentation à l'autorité d'enregistrement d'un document probant ou d'une combinaison de documents et de données biométriques.	

Numéro	Nom	Définition	Affectation
IA-4.4	GESTION DES IDENTIFICATEURS	L'organisation gère les identificateurs d'utilisateur en identifiant de façon unique l'utilisateur comme [Affectation : caractéristique définie par l'organisation identifiant le statut de l'utilisateur].	
IA-5	GESTION DES AUTHENTIFIANTS	(A) L'organisation gère les authentifiants d'utilisateur et de dispositif en vérifiant, au moment de la distribution initiale des authentifiants, l'identité de l'utilisateur et (ou) du dispositif authentifié. (B) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant le contenu initial des authentifiants définis par l'organisation. (C) L'organisation gère les authentifiants d'utilisateur et de dispositif en s'assurant que le mécanisme d'authentification possède la force appropriée à l'utilisation prévue. (D) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant et appliquant les procédures administratives nécessaires (distribution initiale des authentifiants, authentifiants perdus, compromis ou endommagés et révocation des authentifiants. (E) L'organisation gère les authentifiants d'utilisateur et de dispositif en modifiant le contenu par défaut des authentifiants au moment de l'installation du système. (F) L'organisation gère les authentifiants d'utilisateur et de dispositif en établissant les restrictions minimales et maximales de durée et les conditions de réutilisation des authentifiants (le cas échéant). (G) L'organisation gère les authentifiants d'utilisateur et de dispositif en modifiant et (ou) actualisant les authentifiants [Affectation : durée définie par l'organisation par type d'authentifiant]. (H) L'organisation gère les authentifiants d'utilisateur et de dispositif en protégeant le contenu de l'authentifiant contre toute divulgation et modification non autorisées. (I) L'organisation gère les authentifiants d'utilisateur et de dispositif en exigeant des utilisateurs et des dispositifs qu'ils appliquent des mesures spécifiques de protection des authentifiants.	(G) [Ne dépassant pas 180 jours]
IA-5.1	GESTION DES AUTHENTIFIANTS	Authentification axée sur les mots de passe – Le système : (a) Applique un mot de passe de complexité minimale [Affectation : exigences définies par l'organisation concernant la sensibilité à la casse, le nombre de caractères, la combinaison minuscules-majuscules, les lettres minuscules, les chiffres et les caractères spéciaux, incluant les exigences minimales pour chaque type]; (b) Utilise au minimum [Affectation : nombre de caractères modifiables défini par l'organisation] lors de la création de nouveaux mots de passe; (c) Chiffre les mots de passe stockés et en transit; (d) Applique les restrictions minimales et maximales de durée des mots de passe [Affectation : nombre défini par l'organisation pour la durée minimale ou maximale]; et (e) Interdit la réutilisation des mots de passe pendant [Affectation : nombre défini par l'organisation] les générations.	(1) [Sensible à la casse, huit caractères, au moins une lettre majuscule, une lettre minuscule, un chiffre et un caractère spécial]

Numéro	Nom	Définition	Affectation
IA-5.2	GESTION DES AUTHENTIFIANTS	Authentification axée sur l'ICP – Le système : (a) Valide les certificats en créant une voie de certification, incluant de l'information d'état, vers un ancrage de confiance autorisé; (b) Applique la procédure d'accès autorisé à la clé privée correspondante; et (c) Associe l'identité authentifiée au compte de l'utilisateur.	
IA-5.3	GESTION DES AUTHENTIFIANTS	L'organisation exige que la procédure de demande de [Affectation : types d'authentifiant et (ou) authentifiants spécifiques définis par l'organisation] soit effectuée en personne auprès d'une autorité d'enregistrement désignée avec l'autorisation d'un agent désigné de l'organisation (p. ex., un superviseur).	(3) [ID utilisateur et mot de passe]
IA-5.6	GESTION DES AUTHENTIFIANTS	L'organisation protège les authentifiants au niveau de sécurité qui correspond à la sensibilité et à la criticité de l'information et du système d'information concernés.	
IA-5.7	GESTION DES AUTHENTIFIANTS	L'organisation s'assure qu'aucun authentifiant statique chiffré n'est intégré à des applications ou à des scripts d'accès, ni activé par des touches de fonctions.	
IA-6	OCCULTATION DES AUTHENTIFIANTS	(A) Le système d'information occulte les rétroactions d'information durant le processus d'authentification afin de protéger l'information contre de possibles exploitations et (ou) utilisations par des personnes non autorisées.	
IA-7	AUTHENTIFICATION DES MODULES CRYPTOGRAPHIQUES	(A) Le système d'information utilise des mécanismes d'authentification basés sur un module cryptographique qui satisfait aux conseils du CSTC en matière d'authentification.	
IA-8	IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS NON ORGANISATIONNELS)	(A) Le système d'information identifie de façon unique et authentifie les utilisateurs non organisationnels (ou les processus exécutés en leur nom).	
IR-1	POLITIQUE ET PROCÉDURES D'INTERVENTION EN CAS D'INCIDENT	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique d'intervention en cas d'incident formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'intervention en cas d'incident et des contrôles correspondants. (AA) La politique et les procédures d'intervention en cas d'incident de l'organisation facilite l'intégration de niveaux relevés de préparation durant les urgences et les situations de menace des TI élevées, en conformité avec la Norme opérationnelle de sécurité - Niveaux de préparation des installations du gouvernement fédéral du SCT [Référence 13] et la Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8]	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
IR-2	FORMATION SUR LES INTERVENTIONS EN CAS D'INCIDENT	(A) L'organisation assure la formation du personnel concernant ses rôles et responsabilités relativement aux interventions en cas d'incident liées au système d'information. (B) L'organisation offre des cours de recyclage [Affectation : fréquence définie par l'organisation].	(B) Fréquence [à une fréquence ne dépassant par une fois l'an]

Numéro	Nom	Définition	Affectation
IR-3	TESTS ET EXERCICES RELATIFS AUX INTERVENTIONS EN CAS D'INCIDENT	(A) L'organisation teste et (ou) vérifie la capacité d'intervention en cas d'incidents liés au système d'information [Affectation : fréquence définie par l'organisation] en utilisant [Affectation : tests et (ou) exercices définis par l'organisation] pour déterminer l'efficacité des interventions et documenter les résultats.	(A) Fréquence [à une fréquence ne dépassant par une fois l'an]
IR-4	TRAITEMENT DES INCIDENTS	(A) L'organisation met de l'avant une capacité de traitement des incidents de sécurité qui inclut des activités de préparation, de détection et d'analyse, de confinement, d'éradication et de reprise. (B) L'organisation coordonne les activités de traitement des incidents avec les activités de planification d'urgence. (C) L'organisation intègre les leçons apprises au cours des activités de traitement aux procédures d'intervention, à la formation et aux tests et exercices, et applique les résultats obtenus comme il se doit.	
IR-4.1	TRAITEMENT DES INCIDENTS	L'organisation utilise des mécanismes automatisés pour soutenir le processus de traitement des incidents.	
IR-4.3	TRAITEMENT DES INCIDENTS	L'organisation identifie les classes d'incident et définit les mesures d'intervention appropriées pour permettre la continuité de ses missions et fonctions opérationnelles.	
IR-4.4	TRAITEMENT DES INCIDENTS	L'organisation établit une corrélation entre l'information sur les incidents et les interventions individuelles pour obtenir une perspective organisationnelle de la sensibilisation et des interventions en matière d'incident.	
IR-5	SURVEILLANCE DES INCIDENTS	(A) L'organisation piste et documente les incidents de sécurité liés au système d'information.	
IR-5.1	SURVEILLANCE DES INCIDENTS	L'organisation utilise des mécanismes automatisés pour faciliter le pistage des incidents de sécurité et la collecte et l'analyse de l'information sur les incidents.	
IR-6	SIGNALEMENT DES INCIDENTS	(A) L'organisation exige du personnel qu'il signale les incidents de sécurité suspects aux responsables organisationnels des interventions dans les [Affectation : période définie par l'organisation]. (B) L'organisation communique l'information sur les incidents de sécurité aux autorités désignées.	
IR-6.1	SIGNALEMENT DES INCIDENTS	L'organisation utilise des mécanismes automatisés pour faciliter le signalement des incidents de sécurité.	
IR-6.2	SIGNALEMENT DES INCIDENTS	L'organisation communique aux agents concernés de l'organisation les faiblesses, lacunes et (ou) vulnérabilités du système associées aux incidents signalés.	
IR-7	ASSISTANCE POUR LES INTERVENTIONS EN CAS D'INCIDENT	(A) L'organisation fournit les ressources nécessaires au soutien des interventions en cas d'incident, élément essentiel de la capacité d'intervention de l'organisation; ces ressources fournissent des conseils et de l'aide aux utilisateurs du système d'information pour ce qui touche le traitement et le signalement des incidents de sécurité.	

Numéro	Nom	Définition	Affectation
IR-7.2	ASSISTANCE POUR LES INTERVENTIONS EN CAS D'INCIDENT	L'organisation : (a) Établit une relation de coopération directe entre sa capacité d'intervention et la capacité de protection des systèmes d'information de fournisseurs externes; et (b) Communique l'identité des membres de son équipe d'intervention aux fournisseurs externes.	
IR-8	PLAN D'INTERVENTION EN CAS D'INCIDENT	(A) L'organisation développe un plan d'intervention en cas d'incident qui : (a) Permet à l'organisation de pouvoir compter sur une feuille de route pour la mise en œuvre de sa capacité d'intervention; (b) Décrit la structure et l'organisation de la capacité d'intervention; (c) Propose une approche de haut niveau de la façon dont la capacité d'intervention est intégrée à l'ensemble de l'organisation; (d) Répond à ses exigences spécifiques concernant sa mission, sa taille, sa structure et ses fonctions; (e) Définit les incidents qui doivent être signalés; (f) Définit les paramètres de mesure de sa capacité d'intervention; (g) Définit les ressources et le soutien de la direction nécessaires au maintien et à l'évolution de la capacité d'intervention; et (h) Est révisé et approuvé par des agents désignés de l'organisation. (B) L'organisation distribue des copies du plan à [Affectation : liste définie par l'organisation des employés (par nom et (ou) rôle) chargés des interventions et des éléments organisationnels]. (C) L'organisation examine le plan [Affectation : fréquence définie par l'organisation]. (D) L'organisation révise le plan pour tenir compte des changements dont elle a fait l'objet et (ou) de ceux apportés au système, ou des problèmes relevés au cours de la mise en oeuvre, de l'exécution et des tests du plan. (E) L'organisation communique les changements apportés au plan à [Affectation : liste définie par l'organisation des employés (par nom et (ou) rôle) chargés des interventions et des éléments organisationnels].	(C) Fréquence [à une fréquence ne dépassant par une fois l'an]
MA-1	POLITIQUE ET PROCÉDURES DE MAINTENANCE DES SYSTÈMES	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de maintenance des systèmes d'information formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de maintenance des systèmes d'information et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]

Numéro	Nom	Définition	Affectation
MA-2	MAINTENANCE CONTRÔLÉE	(A) L'organisation planifie, exécute, documente et examine les dossiers de maintenance et de réparation des composantes de système en conformité avec les spécifications du fabricant ou du fournisseur et (ou) ses propres exigences. (B) L'organisation contrôle toutes les activités de maintenance, qu'elles soient effectuées sur place ou à distance et que l'équipement soit réparé sur les lieux ou à l'extérieur. (C) L'organisation exige qu'un agent désigné approuve explicitement le retrait du système, ou des composantes, de ses installations aux fins de maintenance ou de réparation à l'extérieur des locaux. (D) L'organisation nettoie l'équipement afin de supprimer toutes les données des supports avant de l'expédier à l'extérieur aux fins de maintenance ou de réparation. (E) L'organisation vérifie tous les contrôles de sécurité potentiellement concernés pour s'assurer qu'ils continuent de fonctionner adéquatement après les activités de maintenance ou de réparation.	
MA-2.1	MAINTENANCE CONTRÔLÉE	L'organisation tient à jour les dossiers de maintenance du système, qui incluent les éléments suivants : (a) Date et heure de la maintenance; (b) Nom de la personne qui effectue la maintenance; (c) Nom de l'escorte, le cas échéant; (d) Description des opérations de maintenance effectuées; et (e) Liste de l'équipement retiré ou remplacé (incluant les numéros d'identification, le cas échéant).	
MA-3	OUTILS DE MAINTENANCE	(A) L'organisation approuve, contrôle et maintient en permanence les outils de maintenance des systèmes d'information et en surveille l'utilisation.	
MA-3.2	OUTILS DE MAINTENANCE	L'organisation vérifie que les supports qui contiennent des programmes de diagnostic et de test sont exempts de code malveillant avant de les utiliser dans le système.	
MA-4	MAINTENANCE EFFECTUÉE À DISTANCE	(A) L'organisation autorise, surveille et contrôle les activités de maintenance et de diagnostic effectuées à distance. (B) L'organisation permet l'utilisation des outils servant à cette fin seulement si elle est conforme à sa politique et documentée dans le plan de sécurité du système d'information. (C) L'organisation utilise des techniques d'identification et d'authentification robustes lors de l'établissement des sessions d'activités de maintenance et de diagnostic effectuées à distance. (D) L'organisation tient à jour des dossiers de ces activités. (E) [Voir la section Améliorations du contrôle.].	
MA-4.1	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation vérifie les sessions d'activités de maintenance et de diagnostic effectuées à distance, et des responsables désignés examinent les dossiers de maintenance des sessions.	
MA-4.2	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation documente, dans le plan de sécurité du système, l'installation et l'utilisation de ces connexions.	

Numéro	Nom	Définition	Affectation
MA-4.3	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation : (a) Exige que les services de maintenance et de diagnostic soient effectués à partir d'un système qui applique un niveau de sécurité aussi élevé que celui du système cible; ou (b) Retire la composante concernée du système avant l'exécution des activités de maintenance et de diagnostic, la nettoie (en supprime toute information organisationnelle) avant de l'expédier à l'extérieur et, une fois les services exécutés, l'inspecte et la nettoie à nouveau (pour en éliminer tout logiciel malveillant et implant indétectable) avant de la reconnecter au système d'information.	
MA-4.4	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation protège ces activités en utilisant un authentifiant robuste étroitement lié à l'utilisateur; elle isole également la session de maintenance des autres sessions de réseau du système, comme suit : (a) Elle sépare physiquement les voies de communication, ou (b) Elle sépare logiquement les voies de communication en recourant à une méthode de chiffrement conforme aux exigences du contrôle SC-13.	
MA-4.5	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation exige : (a) Que le personnel chargé de la maintenance informe [Affectation : liste des employés définie par l'organisation] du moment où les activités sont prévues (c.-à-d., l'heure et la date); et (b) Qu'un agent désigné de l'organisation, possédant des connaissances spécifiques sur la sécurité de l'information et des systèmes d'information, approuve les activités de maintenance.	
MA-4.6	MAINTENANCE EFFECTUÉE À DISTANCE	L'organisation utilise des mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications durant les activités.	
MA-5	PERSONNEL DE MAINTENANCE	(A) L'organisation établit un processus d'autorisation du personnel de maintenance et tient à jour une liste des organisations et des employés autorisés à effectuer ces activités. (B) L'organisation s'assure que le personnel de maintenance possède les autorisations d'accès requises ou désigne un employé de l'organisation qui possède cette autorisation ainsi que les compétences techniques nécessaires pour superviser les travaux.	

Numéro	Nom	Définition	Affectation
MA-5.1	PERSONNEL DE MAINTENANCE	L'organisation a prévu des procédures pour le personnel de maintenance qui ne possède pas les cotes de sécurité appropriées ou qui n'est pas citoyen canadien; ces procédures incluent les exigences suivantes : (a) Le personnel qui ne possède pas les autorisations d'accès, les cotes de sécurité ou les approbations formelles d'accès requises est escorté et surveillé durant l'exécution des activités de maintenance et de diagnostic par des employés de l'organisation techniquement qualifiés et autorisés et qui possèdent les cotes de sécurité et les autorisations d'accès appropriées; (b) Avant que ce personnel puisse entreprendre les activités de maintenance ou de diagnostic, toutes les composantes de stockage d'information volatile du système sont nettoyées, et les supports d'information non volatile sont enlevés ou physiquement déconnectés du système puis rangés dans un endroit sûr; et (c) Dans l'éventualité où une composante ne pourrait être nettoyée, l'organisation applique les procédures prévues dans le plan de sécurité du système.	
MA-6	Maintenance opportune	(A) L'organisation obtient des services de maintenance et (ou) des pièces de rechange pour [Affectation : liste définie par l'organisation des composantes de sécurité critiques de système et (ou) de composantes clés de technologie de l'information] dans les [Affectation : durée définie par l'organisation] qui suivent la panne.	
MP-1	POLITIQUE ET PROCÉDURES DE PROTECTION DES SUPPORTS	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de protection des supports formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection des supports et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
MP-2	ACCÈS AUX SUPPORTS	(A) L'organisation restreint l'accès des [Affectation : types de support numérique et non numérique définis par l'organisation] aux [Affectation : liste des personnes autorisées définie par l'organisation] en conformité avec [Affectation : mesures de sécurité définies par l'organisation].	
MP-2.2	ACCÈS AUX SUPPORTS	Le système utilise des mécanismes cryptographiques pour protéger et restreindre l'accès aux supports numériques portables.	
MP-3	MARQUAGE DES SUPPORTS	(A) L'organisation, en conformité avec ses politiques et procédures, appose sur les supports amovibles et les sorties des systèmes d'information des indications sur les limites de distribution, les mises en garde concernant la manipulation et l'étiquetage de sécurité (le cas échéant) de l'information. (B) L'organisation exempte les [Affectation : liste définie par l'organisation des types de support amovible] de tout marquage pour autant qu'ils demeurent dans [Affectation : locaux contrôlés définis par l'organisation].	

Numéro	Nom	Définition	Affectation
MP-4	ENTREPOSAGE DES SUPPORTS	(A) L'organisation contrôle physiquement et entrepose de manière sécuritaire les [Affectation : types de support numérique et non numérique définis par l'organisation] dans [Affectation : locaux contrôlés définis par l'organisation], en conformité avec le Guide d'équipement de sécurité (G1-001) de la GRC [Référence 16]. (B) L'organisation protège physiquement et entrepose de manière sécuritaire les supports de système d'information classifiée et protégée en attente de leur destruction (sur place ou à l'extérieur) en utilisant de l'équipement, des techniques et des procédures approuvés.	
MP-4.1	ENTREPOSAGE DES SUPPORTS	L'organisation utilise des mécanismes cryptographiques pour protéger l'information entreposée.	
MP-5	TRANSPORT DES SUPPORTS	(A) L'organisation protège et contrôle [Affectation : types de support numérique et non numérique définis par l'organisation] durant leur transport hors des zones contrôlées en utilisant [Affectation : mesures de sécurité définies par l'organisation] en conformité avec la Norme opérationnelle sur la sécurité matérielle du SCT [Référence 7] et la Norme pour le transport ou la transmission de renseignements et de biens de nature délicate (G1-009) de la GRC [Référence 18]. (B) L'organisation demeure responsable des supports durant leur transport hors des zones contrôlées. (C) L'organisation réserve les activités associées au transport de ces supports au personnel autorisé.	
MP-5.2	TRANSPORT DES SUPPORTS	L'organisation documente les activités associées au transport des supports.	
MP-6	NETTOYAGE DES SUPPORTS	(A) L'organisation nettoie les supports numériques et non numériques de système d'information avant leur élimination ou leur transfert hors de son contrôle ou à des fins de réutilisation. (B) L'organisation utilise des mécanismes de nettoyage dont la force et l'intégrité correspondent à la classification ou à la sensibilité de l'information.	
MP-6.1	NETTOYAGE DES SUPPORTS	L'organisation piste, documente et vérifie le nettoyage des supports et les activités d'élimination.	
MP-6.2	NETTOYAGE DES SUPPORTS	L'organisation teste les procédures et l'équipement de nettoyage pour s'assurer de leur bon rendement [Affectation : fréquence définie par l'organisation].	(2) Fréquence [à une fréquence ne dépassant par une fois l'an]
MP-6.3	NETTOYAGE DES SUPPORTS	L'organisation nettoie les dispositifs portables et amovibles avant de les connecter au système d'information dans les situations suivantes : [Affectation : liste définie par l'organisation des circonstances où les dispositifs de stockage portables et amovibles doivent être nettoyés].	
MP-6.4	NETTOYAGE DES SUPPORTS	L'organisation nettoie les supports qui contiennent de l'information sensible en conformité avec les politiques, normes et procédures pertinentes du GC.	
MP-6.6	NETTOYAGE DES SUPPORTS	L'organisation détruit les supports qui ne peuvent être nettoyés.	

Numéro	Nom	Définition	Affectation
PE-1	POLITIQUE ET PROCÉDURES DE PROTECTION PHYSIQUE ET ENVIRONNEMENTALE	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de protection physique et environnementale formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection physique et environnementale et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
PE-2	AUTORISATIONS D'ACCÈS PHYSIQUE	(A) L'organisation développe et tient à jour une liste des employés autorisés à accéder à l'installation qui héberge le système d'information (sauf dans les cas où l'installation est officiellement accessible au public). (B) L'organisation émet des justificatifs d'autorisation. (C) L'organisation examine et approuve la liste d'accès et les justificatifs [Affectation : fréquence définie par l'organisation], et supprime de la liste les employés qui n'ont plus besoin de droit d'accès.	(C) Fréquence [mensuelle]
PE-2.1	AUTORISATIONS D'ACCÈS PHYSIQUE	L'organisation autorise, selon le poste ou le rôle de l'employé, l'accès physique à l'installation qui héberge le système d'information.	
PE-3	CONTRÔLE D'ACCÈS PHYSIQUE	(A) L'organisation applique les autorisations d'accès physique à tous les points d'accès physique (incluant les points d'entrée/sortie désignés) de l'installation qui héberge le système d'information (à l'exclusion des zones de l'installation officiellement désignées accessibles au public). (B) L'organisation vérifie les autorisations d'accès individuelles avant d'accorder l'accès à l'installation. (C) L'organisation contrôle les entrées de l'installation qui héberge le système d'information en recourant à des dispositifs de contrôle d'accès physique et (ou) à des agents de sécurité. (D) L'organisation contrôle l'accès aux zones officiellement désignées accessibles au public en conformité avec les directives d'évaluation des risques de l'organisation. (E) L'organisation protège les clés, les combinaisons et autres dispositifs de contrôle d'accès physique. (F) L'organisation maintient l'inventaire des dispositifs de contrôle d'accès physique [Affectation : fréquence définie par l'organisation]. (G) L'organisation modifie les combinaisons et les clés [Affectation : fréquence définie par l'organisation] lorsque des clés sont perdues, des combinaisons, compromises, ou lorsque des employés sont transférés ou quittent leur poste.	(F) Inventaire des dispositifs physiques [annuelle] (G) Changement des combinaisons et des clés [seulement lorsque les clés sont perdues, que les combinaisons sont compromises ou que les personnes sont mutées ou quittent leur poste]
PE-3.1	CONTRÔLE D'ACCÈS PHYSIQUE	L'organisation applique les autorisations d'accès physique au système indépendamment des contrôles d'accès physique de l'installation.	
PE-3.3	CONTRÔLE D'ACCÈS PHYSIQUE	L'organisation protège et surveille, 24 heures sur 24 et 7 jours sur 7, tous les points d'accès physique de l'installation qui héberge le système d'information et émet des alarmes, le cas échéant.	

Numéro	Nom	Définition	Affectation
PE-3.4	CONTRÔLE D'ACCÈS PHYSIQUE	L'organisation utilise des contenants verrouillables pour protéger [Affectation : composantes de système définies par l'organisation] contre les accès physiques non autorisés.	(4) [A déterminer, ex. baies de centre de données verrouillables]
PE-5	CONTRÔLE D'ACCÈS AUX DISPOSITIFS DE SORTIE	(A) L'organisation contrôle l'accès physique aux dispositifs de sortie de système d'information pour empêcher les personnes non autorisées d'obtenir les sorties.	
PE-6	SURVEILLANCE DE L'ACCÈS PHYSIQUE	(A) L'organisation surveille l'accès physique au système d'information afin de détecter les incidents de sécurité physique et d'y répondre. (B) L'organisation examine les journaux d'accès physique [Affectation : fréquence définie par l'organisation]. (C) L'organisation coordonne les résultats des examens et des enquêtes avec sa capacité d'intervention en cas d'incident.	(B) Fréquence [à une fréquence ne dépassant pas une fois par mois]
PE-6.1	SURVEILLANCE DE L'ACCÈS PHYSIQUE	L'organisation surveille en temps réel les alarmes d'intrusion physique et l'équipement de surveillance.	
PE-7	CONTRÔLE DES VISITEURS	(A) L'organisation contrôle l'accès physique au système d'information en authentifiant les visiteurs avant d'émettre une autorisation d'accès à l'installation qui héberge le système d'information, sauf dans le cas des zones désignées accessibles au public.	
PE-7.1	CONTRÔLE DES VISITEURS	L'organisation escorte les visiteurs et surveille leurs activités, le cas échéant.	
PE-8	DOSSIERS D'ACCÈS	(A) L'organisation maintient des dossiers sur les visiteurs qui accèdent à l'installation où réside le système d'information (sauf dans les cas où l'installation est officiellement accessible au public). (B) L'organisation examine les dossiers [Affectation : fréquence définie par l'organisation].	(B) Fréquence [au moins 90 jours]
PE-8.1	DOSSIERS D'ACCÈS	L'organisation utilise des mécanismes automatisés pour faciliter la tenue à jour et l'examen des dossiers d'accès.	
PE-8.2	DOSSIERS D'ACCÈS	L'organisation tient à jour un dossier de tous les accès physiques, tant des visiteurs que du personnel autorisé.	
PE-9	ÉQUIPEMENT ET CÂBLAGE D'ALIMENTATION	(A) L'organisation protège l'équipement et le câblage d'alimentation du système d'information contre les dommages et la destruction.	
PE-10	ARRÊT D'URGENCE	(A) L'organisation peut, en situation d'urgence, couper l'alimentation du système d'information ou des composantes individuelles. (B) L'organisation place des interrupteurs ou des dispositifs d'arrêt d'urgence dans [Affectation : liste définie par l'organisation des emplacements occupés par le système ou une composante] pour faciliter l'accès en toute sécurité du personnel. (C) L'organisation protège sa capacité d'interruption d'urgence de l'alimentation contre toute activation non autorisée.	
PE-11	ALIMENTATION D'URGENCE	(A) L'organisation prévoit une source temporaire d'alimentation ininterruptible pour faciliter l'arrêt ordonné du système d'information dans l'éventualité d'une perte de la source d'alimentation principale.	

Numéro	Nom	Définition	Affectation
PE-12	ÉCLAIRAGE D'URGENCE	(A) L'organisation utilise et entretient, pour le système d'information, un système automatique d'éclairage d'urgence qui entre en fonction lorsqu'il y a coupure ou interruption de courant; le système éclaire les sorties d'urgence et les chemins d'évacuation dans l'installation.	
PE-12.1	ÉCLAIRAGE D'URGENCE	L'organisation prévoit l'éclairage d'urgence de toutes les zones de l'installation où sont exécutées des fonctions opérationnelles et de mission essentielles.	
PE-13	PROTECTION CONTRE LES INCENDIES	(A) L'organisation utilise et maintient, pour le système d'information, des réseaux et (ou) des dispositifs de détection et d'extinction d'incendie branchés à une source d'alimentation indépendante.	
PE-13.1	PROTECTION CONTRE LES INCENDIES	L'organisation utilise des réseaux et (ou) dispositifs de détection d'incendie qui entrent en fonction automatiquement et informe l'organisation et les intervenants d'urgence dans l'éventualité d'un incendie.	
PE-14	CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ	(A) L'organisation maintient à [Affectation : niveaux acceptables définis par l'organisation] les niveaux de température et d'humidité dans l'installation qui héberge le système d'information. (B) L'organisation surveille les niveaux de température et d'humidité [Affectation : fréquence définie par l'organisation].	
PE-14.1	CONTRÔLE DE LA TEMPÉRATURE ET DE L'HUMIDITÉ	L'organisation utilise des contrôles automatiques de la température et de l'humidité pour empêcher toute fluctuation potentiellement préjudiciable.	
PE-15	PROTECTION CONTRE LES DÉGÂTS D'EAU	(A) L'organisation protège le système d'information contre tout dommage causé par une fuite d'eau en recourant à des vannes d'arrêt accessibles qui fonctionnent adéquatement et dont le personnel concerné connaît l'emplacement.	
PE-16	LIVRAISON ET RETRAIT	(A) L'organisation autorise, surveille et contrôle l'entrée et la sortie dans l'installation des [Affectation : types de composante de système définis par l'organisation] et tient à jour les dossiers pertinents.	
PE-17	LIEU DE TRAVAIL DE SECOURS	(A) L'organisation utilise [Affectation : contrôles de sécurité de gestion, opérationnels et techniques de système définis par l'organisation] dans les lieux de travail de secours. (B) L'organisation évalue dans la mesure du possible l'efficacité des contrôles de sécurité dans les lieux de travail de secours. (C) L'organisation permet aux employés de communiquer avec le personnel chargé de la sécurité de l'information en cas d'incidents ou de problèmes de sécurité.	(A) [Contrôles définis par l'autorisateur]
PE-18	EMPLACEMENT DES COMPOSANTES DE SYSTÈME D'INFORMATION	(A) L'organisation entrepose les composantes de système d'information de manière à réduire tout dommage potentiel de nature physique et environnementale et à réduire les risques d'accès non autorisé.	

Numéro	Nom	Définition	Affectation
PL-1	POLITIQUE ET PROCÉDURES DE PLANIFICATION DE LA SÉCURITÉ	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de planification de la sécurité formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de planification de la sécurité et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
PL-2	PLAN DE SÉCURITÉ DES SYSTÈMES	(A) L'organisation développe pour le système d'information un plan de sécurité qui : (a) Est conforme à l'architecture d'entreprise de l'organisation; (b) Définit explicitement les limites d'autorisation du système; (c) Décrit le contexte opérationnel du système au plan de la mission et des processus opérationnels; (d) Définit les catégories de sécurité du système, incluant la logique sous-jacente; (e) Décrit l'environnement opérationnel du système; (f) Décrit les relations ou les connexions avec les autres systèmes; (g) Donne un aperçu des exigences du contrôle de sécurité du système; (h) Décrit les contrôles de sécurité existants ou prévus pour répondre à ces exigences, y compris la justification des décisions concernant l'adaptation des contrôles et l'identification des contrôles complémentaires; et (i) Sera examiné et approuvé par le responsable de l'autorisation ou un représentant désigné avant la mise en œuvre du plan. (B) L'organisation examine le plan de sécurité du système d'information [Affectation : fréquence définie par l'organisation]. (C) L'organisation met le plan à jour pour tenir compte des changements apportés au système et (ou) à l'environnement d'exploitation, ou des problèmes soulevés lors de la mise en œuvre du plan ou des évaluations des contrôles de sécurité.	(B) Fréquence [selon une période ne dépassant pas une fois tous les quatre ans ou lorsqu'un changement important au système survient]
PL-2.1	PLAN DE SÉCURITÉ DES SYSTÈMES	L'organisation : (a) Développe pour le système d'information un concept d'opération (CONOPS) de sécurité qui inclut, au minimum : (i) le but du système; (ii) une description de l'architecture du système; (iii) le barème d'autorisation de sécurité; et (iv) les catégories de sécurité et les facteurs utilisés pour les déterminer; et (b) Révise et tient à jour le CONOPS [Affectation : fréquence définie par l'organisation].	

Numéro	Nom	Définition	Affectation
PL-2.2	PLAN DE SÉCURITÉ DES SYSTÈMES	L'organisation développe pour le système d'information une architecture fonctionnelle qui identifie et maintient : (a) Les interfaces externes, l'information échangée entre elles et leurs mécanismes de protection; (b) Les rôles d'utilisateur et les privilèges d'accès attribués à chacun; (c) Les exigences uniques des contrôles de sécurité; (d) Les types d'information traités, stockés ou transmis par le système, incluant tout besoin de protection stipulé dans les lois du GC et les politiques, directives et normes concernées du SCT; et (e) La priorité de restauration de l'information ou des services du système.	
PL-5	ÉVALUATION DES FACTEURS RELATIFS À LA VIE PRIVÉE	(A) L'organisation effectue une évaluation des facteurs relatifs à la vie privée du système d'information en conformité avec la Politique d'évaluation des facteurs relatifs à la vie privée du SCT [Référence 25].	
PL-6	PLANIFICATION DES ACTIVITÉS RELATIVES À LA SÉCURITÉ	(A) L'organisation planifie et coordonne les activités liées à la sécurité du système d'information avant de les appliquer afin de réduire leur incidence sur les activités organisationnelles (c.-à-d., mission, fonctions, image et réputation), les biens de l'organisation et les individus.	
PM-1	PLAN DU PROGRAMME DE SÉCURITÉ DE L'INFORMATION	(A) L'organisation développe et diffuse un plan du programme organisationnel de sécurité de l'information qui : (a) Donne un aperçu des exigences du programme et une description des contrôles de gestion des programmes de sécurité et des contrôles communs existants ou prévus pour répondre à ces exigences; (b) Donne suffisamment d'information sur les contrôles de gestion de programme et les contrôles communs (incluant la spécification explicite ou par référence des paramètres d'affectation et de sélection des contrôles) pour permettre une mise en œuvre formellement conforme à l'objectif du plan ainsi que la détermination subséquente des risques potentiels lorsque le plan est mis en œuvre tel que prévu; (c) Inclut de l'information sur la conformité, les rôles, les responsabilités, l'engagement de la direction et la coordination entre les entités organisationnelles; (d) Est approuvé par un cadre supérieur responsable et tenu de rendre compte des risques encourus par les activités (incluant la mission, les fonctions, l'image et la réputation) et les biens de l'organisation, les individus, les autres organisations et le Canada; (B) L'organisation examine le plan du programme organisationnel de sécurité [Affectation : fréquence définie par l'organisation]; et (C) L'organisation révise le plan pour tenir compte des changements organisationnels et des problèmes identifiés durant la mise en œuvre du plan ou les évaluations des contrôles de sécurité.	
PM-2	AGENT PRINCIPAL DE SÉCURITÉ DE L'INFORMATION	(A) L'organisation nomme l'agent principal de sécurité de l'information et lui confie, en même temps que les ressources requises, la mission de coordonner, développer, mettre en œuvre et maintenir le programme organisationnel de sécurité de l'information.	

Numéro	Nom	Définition	Affectation
PM-3	RESSOURCES LIÉES À LA SÉCURITÉ DE L'INFORMATION	(A) L'organisation s'assure que toutes les demandes de planification des immobilisations et des investissements incluent les ressources nécessaires à la mise en œuvre du programme de sécurité et documentent toutes les exceptions à cette exigence; (B) L'organisation effectue une analyse de rentabilisation pour identifier les ressources nécessaires; et (C) L'organisation s'assure que les ressources liées à la sécurité de l'information peuvent être utilisées tel que prévu.	
PM-4	PROCESSUS DES PLANS D'ACTION ET JALONS	(A) L'organisation met en œuvre un processus pour assurer la tenue à jour des plans d'action et des jalons du programme de sécurité et des systèmes d'information organisationnels correspondants et pour documenter les mesures correctives pertinentes d'atténuation des risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada.	
PM-5	INVENTAIRES DES SYSTÈMES D'INFORMATION	(A) L'organisation développe et tient à jour un inventaire de ses systèmes d'information.	
PM-6	MESURES DU RENDEMENT DE LA SÉCURITÉ DE L'INFORMATION	(A) L'organisation développe et surveille les résultats des mesures du rendement de la sécurité de l'information et produit les rapports pertinents.	
PM-7	ARCHITECTURE D'ENTREPRISE	(A) L'organisation développe une architecture d'entreprise en tenant compte de la sécurité de l'information et des risques qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada.	
PM-9	STRATÉGIE DE GESTION DU RISQUE	(A) L'organisation développe une stratégie détaillée de gestion des risques liés à l'exploitation et à l'utilisation des systèmes d'information et qui menacent les activités et les biens de l'organisation, les individus, les autres organisations et le Canada; et (B) L'organisation applique la stratégie de manière uniforme à l'échelle de l'organisation.	
PM-10	PROCESSUS D'AUTORISATION DE SÉCURITÉ	(A) L'organisation gère (c.-à-d., documente, assure le suivi et produit des rapports) la situation des systèmes d'information organisationnels sur le plan de la sécurité en recourant à un processus d'autorisation de sécurité; (B) L'organisation attribue à des individus des rôles et responsabilités spécifiques dans son processus de gestion du risque ; et (C) L'organisation intègre l'ensemble du processus d'autorisation de sécurité à son programme de gestion du risque.	
PS-1	POLITIQUE ET PROCÉDURES DE SÉCURITÉ DU PERSONNEL	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de sécurité du personnel formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de sécurité du personnel et des contrôles correspondants.	(A) (B) Fréquence [au moins une fois l'an]

Numéro	Nom	Définition	Affectation
PS-2	CATÉGORISATION DES POSTES	(A) L'organisation catégorise tous les postes en fonction des préjudices que les individus peuvent causer en commettant des actes malveillants découlant de l'exercice des privilèges associés à leur poste. (B) L'organisation choisit le niveau de filtrage approprié (p. ex., ERC, I, II, III) pour les titulaires des postes. (C) L'organisation examine et révise les catégorisations des postes [Affectation : fréquence définie par l'organisation].	
PS-3	ENQUÊTE DE SÉCURITÉ SUR LE PERSONNEL	(A) L'organisation filtre les individus avant d'autoriser l'accès au système d'information, en conformité avec la Norme sur la sécurité du personnel du SCT [Référence 10]. (B) L'organisation filtre les individus de nouveau lorsque [Affectation : liste définie par l'organisation des conditions qui exigent un nouveau filtrage et fréquence de ce filtrage, le cas échéant].	
PS-4	LICENCIEMENT DU PERSONNEL	(A) L'organisation, lors de la cessation d'emploi d'un individu, met un terme à l'accès du système d'information. (B) L'organisation, lors de la cessation d'emploi d'un individu, effectue des entrevues de fin d'emploi. (C) L'organisation, lors de la cessation d'emploi d'un individu, retire tous les biens de l'organisation associés à la sécurité du système d'information. (D) L'organisation, lors de la cessation d'emploi d'un individu, maintient l'accès à l'information organisationnelle et aux systèmes d'information en conformité avec la Norme sur la sécurité du personnel du SCT [Référence 10].	
PS-5	TRANSFERT DE PERSONNEL	(A) L'organisation examine les autorisations d'accès physique et logique aux systèmes d'information et (ou) aux installations lorsque le personnel est réaffecté ou transféré dans d'autres postes au sein de l'organisation et entreprend des [Affectation : mesures de transfert ou de réaffectation définies par l'organisation] dans les [Affectation : durée définie par l'organisation conformément à la Norme sur la sécurité du personnel du SCT [Référence 10]].	
PS-6	ENTENTES D'ACCÈS	(A) L'organisation s'assure que les individus qui ont besoin d'accéder à l'information organisationnelle et aux systèmes d'information signent les ententes d'accès appropriées avant que l'accès ne leur soit accordé. (B) L'organisation examine et (ou) met à jour les ententes d'accès [Affectation : fréquence définie par l'organisation].	
PS-6.1	ENTENTES D'ACCÈS	L'organisation s'assure que l'accès à l'information visée par des mesures de protection spéciales est accordé uniquement aux individus qui : (a) Possèdent une autorisation d'accès valable attestée par les responsabilités gouvernementales officielles qui leur ont été assignées; et (b) Satisfont aux critères correspondants de sécurité du personnel.	

Numéro	Nom	Définition	Affectation
PS-7	SÉCURITÉ DU PERSONNEL TIERS	(A) L'organisation définit les exigences du contrôle de la sécurité du personnel, incluant les rôles et responsabilités des fournisseurs tiers en matière de sécurité. (B) L'organisation documente les exigences du contrôle de la sécurité du personnel. (C) L'organisation surveille la conformité des fournisseurs. (AA) L'organisation s'assure d'effectuer le filtrage de sécurité des organisations et des individus du secteur privé qui ont accès à l'information et aux biens protégés et classifiés, en conformité avec la Norme sur la sécurité du personnel du SCT [Référence 10]. (BB) L'organisation définit explicitement la surveillance gouvernementale et les rôles et responsabilités d'utilisateur final relativement aux services de tiers, en conformité avec la Norme de sécurité et de gestion des marchés du SCT [Référence 26].	
PS-8	SANCTIONS IMPOSÉES AU PERSONNEL	(A) L'organisation utilise un processus formel de sanctions pour le personnel qui ne se conforme pas aux politiques et procédures établies de sécurité de l'information.	
RA-1	POLITIQUE ET PROCÉDURES D'ÉVALUATION DES RISQUES	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique d'évaluation des risques formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'évaluation des risques et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
RA-2	CATÉGORIES DE SÉCURITÉ	(A) L'organisation catégorise l'information et les systèmes d'information en conformité avec les lois pertinentes du GC et les politiques, directives et normes du SCT. (B) L'organisation documente les résultats de la catégorisation (incluant la logique correspondante) dans le plan de sécurité du système d'information. (C) L'organisation s'assure que les décisions concernant les catégories sont examinées et approuvées par l'agent d'autorisation ou un représentant désigné.	
RA-3	ÉVALUATION DES RISQUES	(A) L'organisation effectue une évaluation des risques, incluant la probabilité et l'ampleur des préjudices, associés aux différents aspects du système d'information (accès non autorisé, utilisation, divulgation, interruption, modification ou destruction) et de l'information qu'il traite, stocke et transmet, en conformité avec la norme Sécurité relative à l'organisation et l'administration du SCT [Référence 14]. (B) L'organisation documente les résultats de l'évaluation dans [Sélection : plan de sécurité; rapport d'évaluation des risques; [Affectation : document défini par l'organisation]]. (C) L'organisation examine les résultats de l'évaluation [Affectation : fréquence définie par l'organisation]. (D) L'organisation effectue une mise à jour de l'évaluation [Affectation : fréquence définie par l'organisation] ou chaque fois que des changements importants sont apportés au système ou à l'environnement d'exploitation (incluant l'identification des nouvelles menaces et vulnérabilités), ou lorsque d'autres conditions sont susceptibles d'influer sur l'état de sécurité du système.	(C) Fréquence [à une fréquence ne dépassant par une fois tous les 3 ans]

Numéro	Nom	Définition	Affectation
RA-5	ANALYSE DES VULNÉRABILITÉS	(A) L'organisation identifie les vulnérabilités dans le système d'information et les applications hébergées [Affectation : fréquence définie par l'organisation et (ou) de manière aléatoire en conformité avec le processus défini par l'organisation] et lorsque de nouvelles vulnérabilités susceptibles d'influer sur le système et (ou) les applications sont identifiées et signalées. (B) L'organisation utilise des outils et des techniques d'analyse des vulnérabilités qui favorisent l'interopérabilité entre eux et les composantes automatisées du processus de gestion des vulnérabilités; à cette fin, elle applique des normes sur les aspects suivants : (a) Relevé des plateformes, des lacunes logicielles et des configurations inappropriées; (b) Formatage de listes de vérification et de procédures de test transparentes; et (c) Mesure des répercussions des vulnérabilités. (C) L'organisation examine les rapports d'analyse des vulnérabilités et les résultats des évaluations des contrôles de sécurité. (D) L'organisation corrige les vulnérabilités légitimes [Affectation : temps de réponse définis par l'organisation] en conformité avec son évaluation des risques. (E) L'organisation partage l'information obtenue du processus d'analyse des vulnérabilités et des évaluations des contrôles avec tout le personnel désigné de l'organisation pour faciliter la suppression de vulnérabilités similaires (c.-à-d., faiblesses ou lacunes systémiques) dans les autres systèmes d'information).	(A) Fréquence [au moins tous les 30 jours] (D) Temps de réponse [dans les 30 jours]
RA-5.2	ANALYSE DES VULNÉRABILITÉS	L'organisation met à jour la liste des vulnérabilités relevées [Affectation : fréquence définie par l'organisation] ou lorsque de nouvelles vulnérabilités sont identifiées et signalées.	(2) Fréquence [immédiatement avant chaque analyse des vulnérabilités]
SA-2	Affectation des ressources	(A) L'organisation identifie les exigences en matière de contrôle de sécurité de l'information pour la planification du processus lié à la mission et aux opérations. (B) L'organisation détermine, documente et affecte les ressources nécessaires pour protéger le processus de contrôle de la planification des immobilisations et des investissements du système d'information. (C) L'organisation établit un poste distinct pour la sécurité de l'information dans la documentation de programmation et de budgétisation de l'organisation. Norme opérationnelle de sécurité - Gestion de la sécurité des technologies de l'information du SCT [Référence 8].	
SA-3	SOUTIEN DU CYCLE DE VIE	(A) L'organisation gère le système d'information en utilisant une méthodologie de cycle de développement des systèmes qui inclut les aspects liés à la sécurité de l'information. (B) L'organisation définit et documente les rôles et responsabilités associés à la sécurité de l'information à tous les stades du cycle de développement des systèmes. (C) L'organisation identifie les personnes auxquelles sont attribués des rôles et des responsabilités associés à la sécurité de l'information.	
SA-7	LOGICIEL INSTALLÉ PAR L'UTILISATEUR	(A) L'organisation applique des règles explicites concernant l'installation de logiciel par les utilisateurs.	

Numéro	Nom	Définition	Affectation
SA-8	PRINCIPES D'INGÉNIERIE DE LA SÉCURITÉ	(A) L'organisation applique les principes d'ingénierie de la sécurité aux spécifications, à la conception, au développement, à la mise en œuvre et à la modification des systèmes d'information.	
SA-10	GESTION DE LA CONFIGURATION PAR LES DÉVELOPPEURS	(A) L'organisation exige que les développeurs et (ou) les intégrateurs de système gèrent la configuration durant la conception, le développement, la mise en œuvre et l'exploitation du système. (B) L'organisation exige que les développeurs et (ou) les intégrateurs de système gèrent et contrôlent les changements apportés au système. (C) L'organisation exige que les développeurs et (ou) les intégrateurs de système mettent en œuvre uniquement les changements qu'elle approuve. (D) L'organisation exige que les développeurs et (ou) les intégrateurs de système documentent les changements approuvés apportés au système. (E) L'organisation exige que les développeurs et (ou) les intégrateurs de système assurent le suivi des lacunes de sécurité et de leurs solutions.	
SA-11	TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS	(A) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), créent et mettent en œuvre un plan de test et d'évaluation de la sécurité. (B) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), mettent en œuvre un processus vérifiable de correction des problèmes pour solutionner les faiblesses et les lacunes relevées durant le processus de test et d'évaluation de la sécurité.. (C) L'organisation exige que les développeurs et (ou) les intégrateurs de système, en consultation avec le personnel chargé de la sécurité (incluant les techniciens en sécurité), documentent les résultats des processus de test et d'évaluation de la sécurité et de correction des lacunes.	
SA-11.1	TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS	L'organisation exige que les développeurs et (ou) les intégrateurs de système utilisent des outils d'analyse de code pour identifier les lacunes logicielles communes et documentent les résultats de l'analyse.	
SA-11.2	TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS	L'organisation exige que les développeurs et (ou) les intégrateurs de système effectuent une analyse des vulnérabilités pour documenter les vulnérabilités, leur potentiel d'exploitation et l'atténuation du risque.	
SA-11.3	TESTS DE SÉCURITÉ EFFECTUÉS PAR LES DÉVELOPPEURS	L'organisation exige que les développeurs et (ou) les intégrateurs de système créent un plan de test et d'évaluation de la sécurité et le mettent en œuvre sous la surveillance d'un agent de vérification et de validation indépendant.	

Numéro	Nom	Définition	Affectation
SC-1	POLITIQUE ET PROCÉDURES DE PROTECTION DES SYSTÈMES ET DES COMMUNICATIONS	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique de protection des systèmes et des communications formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique de protection des systèmes et des communications et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
SC-2	PARTITIONNEMENT DES APPLICATIONS	(A) Le système d'information isole les fonctions d'utilisateur (incluant les services d'interface) de la fonctionnalité de gestion.	
SC-2.1	PARTITIONNEMENT DES APPLICATIONS	Le système empêche l'utilisation de fonctions de gestion dans une interface prévue pour des utilisateurs généraux (non privilégiés).	
SC-5	PROTECTION CONTRE LES DÉNIS DE SERVICE	(A) Le système d'information protège contre les types d'attaques par déni de service suivants ou en limite les effets : [Affectation : liste définie par l'organisation des types d'attaques par déni de service ou renvoi à la source de la liste actuelle].	(A) Lise [liste définie par l'organisation]
SC-7	PROTECTION DES FRONTIÈRES	(A) Le système d'information surveille et contrôle les communications à sa frontière externe et à ses principales frontières internes. (B) Le système d'information se connecte aux réseaux ou aux systèmes externes seulement par des interfaces gérées dotées de mécanismes de protection des frontières répartis en conformité avec les spécifications de l'architecture de sécurité de l'organisation.	
SC-7.1	PROTECTION DES FRONTIÈRES	L'organisation attribue physiquement les composantes des systèmes accessibles au public pour séparer les sous-réseaux par des interfaces de réseau physique distinctes.	
SC-7.2	PROTECTION DES FRONTIÈRES	Le système empêche tout accès public aux réseaux internes de l'organisation sauf dans le cas où l'accès est négocié de manière appropriée par des interfaces gérées dotées de dispositifs de protection des frontières.	
SC-7.3	PROTECTION DES FRONTIÈRES	L'organisation limite le nombre de points d'accès au système afin d'exercer une meilleure surveillance des communications entrantes et sortantes et du trafic réseau.	
SC-7.4	PROTECTION DES FRONTIÈRES	L'organisation : (a) Applique une interface gérée à chaque service de télécommunications externe; (b) Établit une politique de flux de trafic pour chaque interface gérée; (c) Utilise des contrôles de sécurité au besoin pour protéger la confidentialité et l'intégrité de l'information transmise; (d) Documente chaque exception à la politique de flux de trafic; elle indique l'exigence (de la mission et (ou) de l'activité opérationnelle) à l'origine de l'exception ainsi que sa durée; (e) Examine les exceptions à la politique de flux de trafic [Affectation : fréquence définie par l'organisation]; et (f) Supprime les exceptions à la politique de flux de trafic qui ne sont plus justifiées par une exigence de mission ou opérationnelle explicite.	(4)(e) Fréquence [à une fréquence ne dépassant par une fois l'an]

Numéro	Nom	Définition	Affectation
SC-7.5	PROTECTION DES FRONTIÈRES	Le système, au niveau des interfaces gérées, interdit tout trafic réseau par défaut et ne l'autorise qu'exceptionnellement (c.-à-d., interdire tout trafic, permettre le trafic par exception).	
SC-7.6	PROTECTION DES FRONTIÈRES	L'organisation empêche toute diffusion d'information non autorisée hors des frontières du système ou toute communication non autorisée par les frontières du système en cas de défaillance opérationnelle des mécanismes de protection des frontières.	
SC-7.7	PROTECTION DES FRONTIÈRES	Le système empêche les dispositifs distants, qui ont établi une connexion non distante avec le système, de communiquer à l'extérieur de cette voie de communication avec les ressources des réseaux externes.	
SC-7.8	PROTECTION DES FRONTIÈRES	Le système achemine [Affectation : trafic de communications externe défini par l'organisation] vers [Affectation : réseaux externes définis par l'organisation] par des serveurs mandataires authentifiés dans les interfaces gérées des dispositifs de protection des frontières.	(8) Liste [liste des communications] (8) Liste [liste des réseaux externes]
SC-7.9	PROTECTION DES FRONTIÈRES	Le système, au niveau des interfaces gérées, interdit le trafic réseau et identifie les utilisateurs internes (ou le code malveillant) qui représentent une menace pour les systèmes externes.	
SC-7.11	PROTECTION DES FRONTIÈRES	Le système vérifie les communications entrantes pour s'assurer qu'elles proviennent d'une source autorisée et qu'elles sont acheminées vers une destination autorisée.	
SC-7.12	PROTECTION DES FRONTIÈRES	Le système applique des mécanismes de protection des frontières intégrés à l'hôte pour les serveurs, les postes de travail et les dispositifs mobiles.	
SC-7.13	PROTECTION DES FRONTIÈRES	L'organisation isole les [Affectation : outils, mécanismes et composantes de soutien clés de sécurité de l'information définis par l'organisation] des autres composantes internes de système par des sous-réseaux physiques distincts dotés d'interfaces gérées avec les autres parties du système.	
SC-8	INTÉGRITÉ DES TRANSMISSIONS	(A) Le système d'information protège l'intégrité de l'information transmise.	
SC-8.1	INTÉGRITÉ DES TRANSMISSIONS	L'organisation utilise des mécanismes cryptographiques pour déceler toute modification apportée à l'information durant sa transmission, sauf si elle est protégée par des mesures physiques de secours. La cryptographie doit être conforme aux exigences du contrôle SC-13.	
SC-9	CONFIDENTIALITÉ DES TRANSMISSIONS	(A) Le système d'information protège la confidentialité de l'information transmise.	
SC-9.1	CONFIDENTIALITÉ DES TRANSMISSIONS	L'organisation utilise des mécanismes cryptographiques pour déceler toute modification apportée à l'information durant sa transmission, sauf si elle est protégée par [Affectation : mesures physiques de secours définies par l'organisation]. La cryptographie doit être conforme aux exigences du contrôle SC-13.	(1) Liste [mesures physiques de secours]
SC-10	DÉCONNEXION DE RÉSEAU	(A) Le système d'information met un terme à toute connexion réseau associée à une session de communications à la fin de la session ou après [Affectation : durée définie par l'organisation] d'inactivité.	(A) [pas plus de 24 heures pour les déconnexions de réseau; pas plus d'une heure pour les sessions utilisateur]
SC-12	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	(A) L'organisation établit et gère les clés de chiffrement utilisées pour les opérations de cryptographie requises dans le système d'information.	

Numéro	Nom	Définition	Affectation
SC-12.1	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	L'organisation maintient la disponibilité de l'information dans l'éventualité où les utilisateurs perdent leurs clés de chiffrement.	
SC-12.2	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	L'organisation produit, contrôle et distribue les clés de chiffrement symétriques en utilisant une technologie et des processus de gestion des clés approuvés par le CSTC.	
SC-12.3	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	L'organisation produit, contrôle et distribue les clés de chiffrement symétriques et asymétriques en utilisant une technologie et des processus de gestion des clés approuvés par le CSTC.	
SC-12.4	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	L'organisation produit, contrôle et distribue les clés de chiffrement asymétriques en utilisant des certificats approuvés d'assurance de niveau moyen ou du matériel de chiffrement prépositionné.	
SC-12.5	ÉTABLISSEMENT ET GESTION DES CLÉS DE CHIFFREMENT	L'organisation produit, contrôle et distribue les clés de chiffrement asymétriques en utilisant des certificats approuvés d'assurance de niveau moyen ou élevé et des jetons de sécurité matériels qui protègent la clé privée de l'utilisateur.	
SC-13	UTILISATION DE LA CRYPTOGRAPHIE	(A) Le système d'information applique des protections cryptographiques fondées sur des systèmes de chiffrement conformes aux lois du GC et aux politiques, directives et normes concernées du SCT.	
SC-13.1	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise, au minimum, la cryptographie validée par le PVMC pour protéger les données non classifiées.	
SC-13.3	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise, au minimum, une cryptographie validée par le PVMC pour protéger les données qui doivent être mises hors de la portée des individus qui possèdent la cote de sécurité appropriée mais non les autorisations d'accès requises.	
SC-13.4	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise une cryptographie [Sélection : validée par le PVMC; approuvée par le CSTC] pour l'application des signatures numériques.	[Validée par le PVMC]
SC-13.100	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise une cryptographie validée par le PVMC pour protéger les données protégées A en transmission.	
SC-13.101	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise cryptographie validée par le PVMC pour protéger les données protégées B en transmission.	
SC-13.103	UTILISATION DE LA CRYPTOGRAPHIE	L'organisation utilise une cryptographie [Sélection : validée par le PVMC; approuvée par le CSTC] pour protéger les données [Sélection : données définies par l'organisation] inactives.	
SC-14	PROTECTION DE L'ACCÈS PUBLIC	(A) Le système d'information protège l'intégrité et la disponibilité de l'information et des applications accessibles au public.	
SC-15	DISPOSITIFS D'INFORMATIQUE COOPÉRATIVE	(A) Le système d'information interdit l'activation à distance des dispositifs d'informatique coopérative, sauf dans les situations suivantes : [Affectation : exceptions définies par l'organisation pour lesquelles l'activation à distance doit être permise]. (B) Le système d'information indique de manière explicite l'utilisation permise de ces dispositifs par ceux qui se trouvent à proximité physique de la ressource.	(A) [aucune exception]
SC-17	CERTIFICATS D'INFRASTRUCTURE À CLÉ PUBLIQUE	(A) L'organisation émet des certificats à clé publique en vertu de la [Affectation : politique de certification définie par l'organisation] ou les obtient en vertu d'une politique de certification appropriée d'un fournisseur de services autorisé.	

Numéro	Nom	Définition	Affectation
SC-18	CODE MOBILE	(A) L'organisation définit le code mobile et les technologies de code mobile acceptables et inacceptables. (B) L'organisation définit les restrictions d'utilisation et donne des conseils sur l'utilisation du code mobile et des technologies de code mobile acceptables. (C) L'organisation autorise, surveille et contrôle l'utilisation du code mobile dans le système d'information.	
SC-18.1	CODE MOBILE	Le système applique des mécanismes de détection et d'inspection pour identifier le code mobile non autorisé et prendre des mesures correctrices, le cas échéant.	
SC-18.2	CODE MOBILE	L'organisation veille à ce que l'acquisition, le développement et (ou) l'utilisation de code mobile qui sera déployé dans les systèmes répondent aux [Affectation : exigences définies par l'organisation concernant le code mobile].	
SC-18.3	CODE MOBILE	Le système empêche le téléchargement et l'exécution de tout code mobile interdit.	
SC-18.4	CODE MOBILE	Le système empêche l'exécution automatique de code mobile dans [Affectation : applications logicielles définies par l'organisation] et exige que [Affectation : mesures définies par l'organisation] soient prises avant d'exécuter le code.	(4) Liste [applications logicielles] (4) Liste [mesures]
SC-20	SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE (SOURCE AUTORISÉE)	(A) Le système d'information produit des éléments additionnels d'information sur l'origine et l'intégrité des données en plus des données faisant autorité qu'il retourne en réponse aux demandes de résolution de nom et d'adresse.	
SC-20.1	SERVICE SÉCURISÉ DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE (SOURCE AUTORISÉE)	Le système, lorsqu'il est utilisé dans un espace de nom hiérarchique distribué, offre des moyens d'indiquer l'état de sécurité des sous-espaces enfants et (si l'enfant offre des services sécurisés de résolution) de vérifier l'existence d'une chaîne de confiance entre les domaines parents et enfants.	
SC-22	ARCHITECTURE ET FOURNITURE DE SERVICE DE RÉSOLUTION DE NOM ET (OU) D'ADRESSE	(A) Les systèmes d'information qui offrent collectivement des services de résolution de nom et d'adresse pour une organisation sont tolérants aux pannes et appliquent une séparation des rôles internes et externes.	
SC-23	AUTHENTICITÉ DES SESSIONS	(A) Le système d'information prévoit des mécanismes pour protéger l'authenticité des sessions de communications.	
SC-23.1	AUTHENTICITÉ DES SESSIONS	Le système invalide les identificateurs de session lorsque l'utilisateur se déconnecte ou à la fin des sessions.	
SC-23.2	AUTHENTICITÉ DES SESSIONS	Le système offre automatiquement une capacité de déconnexion lorsque l'utilisateur recourt à l'authentification pour accéder à des pages Web.	
SC-23.3	AUTHENTICITÉ DES SESSIONS	Le système produit un identificateur de session unique pour chaque session et reconnaît uniquement les identificateurs qu'il produit.	
SC-28	PROTECTION DE L'INFORMATION INACTIVE	(A) Le système d'information protège la confidentialité et l'intégrité de l'information inactive.	
SC-28.1	PROTECTION DE L'INFORMATION INACTIVE	L'organisation utilise des mécanismes cryptographiques pour empêcher la divulgation et la modification non autorisées de l'information inactive qui n'est pas déjà protégée par des mesures physiques de secours. La cryptographie est conforme aux exigences du contrôle SC-13.	

Numéro	Nom	Définition	Affectation
SC-32	PARTITIONNEMENT DES SYSTÈMES D'INFORMATION	(A) L'organisation partitionne au besoin le système d'information en composantes hébergées dans des domaines (ou environnements) physiques distincts.	
SI-1	POLITIQUE ET PROCÉDURES D'INTÉGRITÉ DE L'INFORMATION ET DES SYSTÈMES	(A) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] une politique d'intégrité de l'information et des systèmes formelle et documentée qui définit les divers aspects de la sécurité (but, portée, rôles, responsabilités, engagement de la direction, coordination entre les entités organisationnelles, et conformité). (B) L'organisation développe, diffuse et examine et (ou) met à jour [Affectation : fréquence définie par l'organisation] des procédures formelles et documentées pour faciliter la mise en œuvre de la politique d'intégrité de l'information et des systèmes et des contrôles correspondants.	(A) (B) Fréquence [à une fréquence ne dépassant par une fois l'an]
SI-2	CORRECTION DES LACUNES	(A) L'organisation identifie, signale et corrige les lacunes du système d'information. (B) L'organisation, avant leur installation, teste les rustines logicielles de correction des lacunes pour en vérifier l'efficacité et les répercussions potentielles sur ses systèmes d'information. (C) L'organisation intègre le mécanisme de correction des lacunes à son processus de gestion de la configuration.	
SI-3	PROTECTION CONTRE LE CODE MALVEILLANT	(A) L'organisation utilise des mécanismes de protection contre le code malveillant aux points d'entrée et de sortie du système d'information et dans les postes de travail, les serveurs ou les dispositifs mobiles du réseau afin de détecter et d'éradiquer le code : (a) Transmis par les pièces jointes de courrier électronique, les accès Web, les supports amovibles ou autres sources usuelles; ou (b) Inoculé par l'exploitation des vulnérabilités du système d'information. (B) L'organisation modifie les mécanismes de protection contre le code malveillant (incluant les définitions de signature) dès la diffusion des mises à jour, en conformité avec sa politique et ses procédures de gestion de l'information. (C) L'organisation configure les mécanismes de protection contre le code malveillant de manière à : (a) Effectuer des analyses périodiques du système d'information [Affectation : fréquence définie par l'organisation] et des balayages en temps réel des fichiers de sources externes lors de leur téléchargement, de leur ouverture ou de leur exécution, en conformité avec sa politique de sécurité; et (b) [Sélection (un ou plusieurs) : bloque le code malveillant; met le code malveillant en quarantaine, envoie une alerte à l'administrateur; [Affectation : mesure définie par l'organisation]] lors de la détection de code malveillant. (D) L'organisation traite les faux positifs résultant de la détection et de l'éradication de code malveillant et leurs répercussions potentielles sur la disponibilité du système d'information.	(C) (a) Fréquence [au moins tous les 30 jours] (C) (b) Sélection [met le code malveillant en quarantaine], mesures [mesures]
SI-3.1	PROTECTION CONTRE LE CODE MALVEILLANT	L'organisation centralise la gestion des mécanismes de protection contre le code malveillant.	
SI-3.2	PROTECTION CONTRE LE CODE MALVEILLANT	Le système met automatiquement à jour les mécanismes de protection contre le code malveillant (incluant les définitions de signature).	

Numéro	Nom	Définition	Affectation
SI-3.3	PROTECTION CONTRE LE CODE MALVEILLANT	Le système empêche les utilisateurs non privilégiés de contourner les mécanismes de protection contre le code malveillant.	
SI-4	SURVEILLANCE DES SYSTÈMES D'INFORMATION	(A) L'organisation surveille les événements liés au système d'information en conformité avec [Affectation : objectifs de surveillance définis par l'organisation] et détecte les attaques contre le système. (B) L'organisation identifie les utilisations non autorisées du système d'information. (C) L'organisation déploie dans le système d'information des dispositifs de surveillance à la fois (i) stratégiquement pour collecter l'information qu'elle juge essentielle et (ii) de manière aléatoire pour pister des types de transaction qui l'intéressent particulièrement. (D) L'organisation relève le niveau des activités de surveillance du système d'information chaque fois qu'elle identifie un risque accru pour les activités et les biens de l'organisation, les individus, les autres organisations ou le Canada suite à la réception de renseignements, d'information concernant le respect des lois ou d'information en provenance d'autres sources crédibles. (E) L'organisation obtient un avis juridique concernant les activités de surveillance du système d'information en conformité avec les lois du GC et les politiques, directives et normes du SCT.	(A) Liste [liste des objectifs définie par l'autorisateur]
SI-4.1	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise des protocoles communs pour interconnecter et configurer les outils individuels de détection en un mécanisme de détection d'intrusion systémique unique.	
SI-4.2	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise des outils automatisés pour effectuer une analyse des événements en temps quasi réel.	
SI-4.3	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise des outils automatisés pour intégrer les outils de détection d'intrusion aux mécanismes de contrôle d'accès et de flux pour contrer rapidement les attaques; les mécanismes peuvent alors être reconfigurés de manière à permettre l'isolation et l'élimination des attaques.	
SI-4.4	SURVEILLANCE DES SYSTÈMES D'INFORMATION	Le système surveille les communications entrantes et sortantes pour détecter toute activité ou condition inhabituelles ou non autorisées.	
SI-4.7	SURVEILLANCE DES SYSTÈMES D'INFORMATION	Le système informe [Affectation : liste définie par l'organisation des employés (identifiés par nom et (ou) rôle) chargés d'intervenir en cas d'incident] des événements suspects et prend les [Affectation : liste définie par l'organisation des mesures les moins nuisibles d'interruption des événements suspects].	(7) Liste [liste des rôles], liste [liste des mesures d'interruption]
SI-4.8	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation protège l'information obtenue des outils de surveillance des intrusions contre tout accès non autorisé et toute modification et suppression.	
SI-4.9	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation teste et (ou) vérifie la capacité des outils de surveillance des intrusions [Affectation : période définie par l'organisation].	
SI-4.11	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation analyse le trafic des communications sortantes à la frontière externe du système (c.-à-d., à son périmètre) et, le cas échéant, à certains de ses points intérieurs (p. ex., sous-réseaux, sous-systèmes) pour découvrir des anomalies.	

Numéro	Nom	Définition	Affectation
SI-4.12	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise des mécanismes automatisés pour alerter le personnel de sécurité des répercussions potentielles des activités inhabituelles ou inappropriées suivantes : [Affectation : liste définie par l'organisation des activités inhabituelles ou inappropriées qui déclenchent des alertes].	(12) Liste [liste des activités inhabituelles ou inappropriées qui déclenchent des alertes]
SI-4.14	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise un système de détection d'intrusions sans fil pour identifier les dispositifs sans fil indésirables et détecter les tentatives d'attaque et les compromissions et (ou) brèches potentielles du système.	
SI-4.15	SURVEILLANCE DES SYSTÈMES D'INFORMATION	L'organisation utilise un système de détection d'intrusions pour surveiller le trafic de communications sans fil lors de son passage dans le circuit des réseaux.	
SI-5	DIRECTIVES, ALERTES ET AVIS DE SÉCURITÉ	(A) L'organisation reçoit régulièrement d'organisations externes désignées des alertes, avis et directives concernant le système d'information. (B) L'organisation produit les alertes, avis et directives de sécurité internes qu'elle juge nécessaires. (C) L'organisation diffuse des alertes, avis et directives de sécurité à [Affectation : liste des employés (par nom et (ou) rôle) définie par l'organisation]. (D) L'organisation applique des directives de sécurité à des intervalles prédéterminés ou informe les organisations émettrices du niveau de non-conformité.	(C) Liste [liste des rôles]
SI-7	INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL	(A) Le système d'information détecte les modifications non autorisées du logiciel et de l'information.	
SI-7.1	INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL	L'organisation réévalue l'intégrité du logiciel et de l'information en effectuant [Affectation : fréquence définie par l'organisation] des analyses d'intégrité du système.	(1) Fréquence [à une fréquence ne dépassant pas 30 jours]
SI-7.2	INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL	L'organisation utilise des outils automatisés qui produisent des avis aux employés désignés lors de la découverte d'écarts durant la vérification de l'intégrité.	
SI-7.3	INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL	L'organisation utilise des outils de vérification de l'intégrité gérés centralement.	
SI-7.4	INTÉGRITÉ DE L'INFORMATION ET DU LOGICIEL	L'organisation exige l'utilisation d'emballages inviolables pour les [Affectation : composantes de système définies par l'organisation] durant [Sélection : transport du fournisseur au site opérationnel; durant l'exploitation; les deux].	(4) Liste [composantes de système d'information], sélection [transport du fournisseur au site opérationnel et durant l'exploitation]
SI-9	RESTRICTIONS RELATIVES À LA SAISIE D'INFORMATION	(A) L'organisation limite au personnel autorisé la capacité d'entrer de l'information dans le système.	
SI-10	VALIDATION DE LA SAISIE D'INFORMATION	(A) Le système d'information vérifie la validité des entrées d'information.	

Numéro	Nom	Définition	Affectation
SI-11	TRAITEMENT DES ERREURS	(A) Le système d'information identifie les conditions d'erreur potentielles liées à la sécurité. (B) Le système d'information produit des messages d'erreur qui incluent l'information nécessaire sur les mesures correctrices sans révéler [Affectation : information sensible ou potentiellement préjudiciable définie par l'organisation] contenue dans les journaux d'erreurs et les messages administratifs qui pourrait être exploitée par des adversaires. (C) Le système d'information révèle les messages d'erreur seulement au personnel autorisé.	(B) [Information sensible ou préjudiciable définie par l'autorisateur]
SI-12	TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION	(A) L'organisation traite et conserve l'information interne et celle produite par le système d'information en conformité avec les lois du GC, les politiques, directives et normes concernées du SCT et les exigences opérationnelles.	