Exigences en matière de sécurité de la technologie de l'information

Traitement des renseignements de nature délicate dans les locaux de l'entrepreneur

Date de publication : 11 juin 2012

Table des matières

Introduction

1.1 Objectif

L'objectif du présent document est de préciser les exigences en matière de sécurité de la technologie de l'information (STI) relatives au traitement de renseignements de nature délicate de la Commission de l'immigration et du statut de réfugié du Canada (CISR) dans les locaux de l'entrepreneur. Les exigences en matière de STI prévoient un minimum de mesures de protection de la sécurité à mettre en œuvre pour veiller à la protection nécessaire de l'information.

Le présent document vise à aider l'entrepreneur à atteindre un niveau de sécurité minimal compte tenu des principes et des exigences de la Politique sur la sécurité du gouvernement (PSG) et des directives, des lignes directrices et des normes connexes du gouvernement du Canada (GC).

Le document doit servir de référence à l'entrepreneur pour préparer une réponse à une demande de propositions (DP) au cours d'un processus d'approvisionnement. Lorsqu'un contrat est attribué, un examen indépendant de la STI est effectué par un coordonnateur de la sécurité de la TI (CSTI) de la CISR pour que l'entrepreneur puisse être autorisé à faire la collecte, le traitement et le stockage des renseignements de nature délicate de la CISR dans ses locaux.

1.2 Priorité

Les exigences en matière de sécurité visent à garantir la **confidentialité** de l'information recueillie, traitée et stockée dans les locaux de l'entrepreneur. La PSG entend par confidentialité la qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées, afin de prévenir tout préjudice à l'intérêt national ou à d'autres intérêts; le terme renvoie à des dispositions précises de la *Loi sur l'accès à l'information* et de la *Loi sur la protection des renseignements personnels*.

1.3 Portée

Les renseignements de nature délicate traités dans les locaux de l'entrepreneur doivent l'être comme dans une installation de la CISR. Les exigences en matière de STI sont conçues pour protéger la confidentialité des fonds de renseignements de la CISR dont la cote de sécurité est désignée **Protégé B** ou de niveau inférieur. La ligne directrice relative à l'identification des biens, publiée par le Secrétariat du Conseil du Trésor (SCT), prévoit que si la confidentialité de l'information désignée Protégé B est compromise, il est raisonnable de s'attendre à ce que la divulgation cause un grave préjudice à des intérêts privés ou étrangers. Selon le cas, l'entrepreneur principal est responsable de veiller à ce que tous les sous-traitants respectent toutes les exigences définies aux présentes.

1.4 Méthode

Les exigences en matière de STI sont fondées sur les politiques, les directives, les lignes directrices et les normes du gouvernement du Canada. Les exigences sont principalement tirées du document du SCT intitulé Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information (GSTI) et du Guide de la gestion des risques d'atteinte à la sécurité des technologies de l'information (MG-2) publié par le Centre de la sécurité des télécommunications Canada (CSTC).

2. Organisation de l'entrepreneur et contrôle de sécurité

La sécurité repose sur de nombreuses couches de protection; c'est-à-dire que, pour garantir la protection efficace de l'information, les exigences en matière de STI doivent être précédées et appuyées par d'autres aspects de la sécurité et des politiques connexes. Les mesures de protection relatives à la sécurité cernées dans la présente section doivent être en place **avant** la mise en œuvre des mesures de protection en matière de STI définies à la Section 3.

2.1 Organisation de la sécurité

L'entrepreneur doit nommer un agent de sécurité d'entreprise (ASE) et un agent de sécurité d'entreprise intérimaire (ASEI).

L'ASE est responsable de l'élaboration, de la mise en œuvre, de la mise à jour, de la coordination et de la vérification des politiques, des normes et des procédures en matière de sécurité d'entreprise pour vérifier les éléments suivants :

- Les membres du personnel chargé du traitement des renseignements de nature délicate détiennent une autorisation de sécurité adéquate et ont fait l'objet d'un contrôle;
- la sécurité physique est conforme;
- la sécurité des TI est conforme.

À la demande de la CISR, le nom et les coordonnées de l'ASE seront fournis à l'agent de sécurité organisationnel (ASO) de la CISR, qui se chargera d'aviser le CSTI.

Tous les ASE et les ASEI sont tenus d'assister à une séance de formation et de sensibilisation à la sécurité organisée et offerte par l'ASO et le CSTI de la CISR.

2.2 Vérification de la sécurité physique par TPSGC

Les mesures de protection en matière de STI et leur mise en place, décrites dans le présent document, sont fondées sur l'exigence obligatoire selon laquelle les lieux physiques de l'entrepreneur ont été inspectés, certifiés et accrédités à des fins de traitement et de stockage de renseignements de nature délicate par la Direction de la sécurité industrielle canadienne (DSIC) ainsi que Travaux publics et Services gouvernementaux Canada (TPSGC). L'entrepreneur doit obtenir et détenir une attestation de vérification d'organisation désignée (VOD) valide délivrée par la DSIC.

L'ASO de la CISR vérifiera auprès de la DSIC que l'VOD est valide et avisera le CSTI de la CISR avant qu'un examen de la sécurité des TI ne soit effectué.

2.3 Sécurité du personnel

Tous les membres du personnel de l'entrepreneur qui ont accès aux renseignements de nature délicate de la CISR doivent détenir une **cote de fiabilité** (attestation de sécurité) valide. Les personnes auxquelles on a accordé une attestation de sécurité n'auront accès à l'information, aux biens ou aux établissements protégés qu'en fonction du besoin de savoir.

L'ASO de la CISR, ou son délégué, vérifiera l'attestation de sécurité de tous les membres du personnel de l'entrepreneur et rendra compte au CSTI de la CISR.

Tous les membres du personnel responsables du traitement des renseignements de nature délicate de la CISR doivent d'abord assister à une séance de formation et de sensibilisation à la sécurité organisée et offerte par l'ASC avant que l'accès à l'information ne leur soit accordé.

2.4 Traitement électronique des données – production de documents et de données

À la suite de l'attribution d'un contrat à un entrepreneur par TPSGC ou la CISR visant le traitement électronique d'information protégée dans le système de TI de l'entrepreneur, ce dernier doit demander au CSTI d'effectuer un examen de la production de documents et de données dans le cadre du Traitement électronique des données (TED).

Un rapport faisant état de recommandations et de suggestions sera préparé par le CSTI et envoyé à l'ASE de l'organisation. L'application des recommandations est obligatoire, et toutes suggestions, quoique non impératives, devraient être prises en considération dans les correctifs subséquents.

L'ASO de la CISR, ou son délégué, vérifiera l'examen de la production de documents et de données dans le cadre du TED et rendra compte au CSTI de la CISR.

2.5 Sécurité de l'information

Tous les documents sur support papier et tous les documents enregistrés sur un support numérique (p. ex. DC/DVD) doivent être traités et transportés conformément aux directives et aux lignes directrices du GC. Tous les documents sur support papier et autres supports doivent porter la mention appropriée de classification de sécurité de la CISR. Toute lettre d'accompagnement, tout formulaire d'accompagnement ou bordereau de circulation doivent porter la mention du plus haut niveau de classification des documents joints.

Le transport d'information liée au présent contrat à destination ou en provenance de l'établissement physique de l'entrepreneur doit être conforme au guide Transport et transmission de renseignements protégés ou classifiés (G1-009) de la GRC.

2.6 Surveillance de la conformité en matière de sécurité

La CISR conserve le droit de mener des inspections régulières ou périodiques, dont la fréquence sera déterminée par l'ASO ou le CSTI, des locaux de l'entrepreneur pour veiller à la conformité avec les politiques du GC relatives au transport, au stockage et au traitement des renseignements de nature délicate de la CISR.

3. Contrôles de sécurité de la technologie de l'information

Un catalogue de contrôle de sécurité est une source unique pour une série de contrôles de sécurité de base (p. ex. mesures de protection ou contre-mesures) qui peuvent être déployés pour protéger la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Le catalogue a été élaboré par le CSTC, qui s'est fondé sur le contenu de la publication spéciale 800-53 du National Institute of Science and Technology (NIST) : Recommended Security Controls for Federal Information Systems (contrôles de sécurité recommandés pour les systèmes d'information fédéraux). Les définitions des contrôles de sécurité du catalogue ont été modifiées et étoffées en fonction du contexte du GC.

Le processus employé pour adapter les exigences en matière de sécurité à un système d'information comprend la catégorisation et l'adaptation des contrôles de sécurité. Les familles et les classes de contrôles de sécurité ont été adaptées dans la section suivante pour privilégier la protection de la confidentialité de l'information. Le nouvel ensemble de contrôles de sécurité qui découle du processus d'adaptation s'intitule « contrôles de sécurité sur mesure ». Les contrôles de sécurité sur mesure à l'intention de l'entrepreneur qui détient des renseignements de nature délicate de la CISR portant la mention Protégé B ou une cote de sécurité inférieure se trouvent à l'annexe B.

Il existe deux classes générales de contrôles de sécurité – opérationnelle et technique – tirées du catalogue de contrôle de sécurité, qui jettent les bases des exigences en matière de sécurité visant la protection de la confidentialité des produits d'information. Voici les définitions des deux différentes classes de contrôles de sécurité :

a. **Contrôles de sécurité opérationnelle** – Contrôles de sécurité (p. ex. mesures de protection ou contre-mesures) de tout système d'information qui sont principalement appliqués et exécutés par des personnes (et non par des systèmes);

b. **Contrôles de sécurité technique** – Contrôles de sécurité (p. ex. mesures de protection ou contre-mesures) d'un système d'information qui sont principalement appliqués et exécutés par le système d'information au moyen de mécanismes faisant partie du matériel, des logiciels ou des micrologiciels du système.

Chaque classe de contrôles de sécurité (p. ex. opérationnelle et technique) est divisée en familles de contrôles de sécurité. La classe opérationnelle est composée des familles suivantes :

a. **Sensibilisation et formation (SF)** – contrôles de sécurité qui ont trait à l'éducation et à la sensibilisation des utilisateurs quant à la sécurité du système d'information;

b. **Réaction aux incidents (RI)** – contrôles de sécurité qui appuient la détection et l'établissement de rapports d'incidents ainsi que la réaction aux incidents en matière de sécurité survenus dans le système d'information;

c. **Protection des supports (PS)** – contrôles de sécurité qui garantissent la protection des supports du système d'information (c.-à-d. les disques, les bandes magnétiques, etc.) tout au long de leur cycle de vie;

d. **Sécurité du personnel (SP**) – contrôles de sécurité qui mettent en place les procédures nécessaires pour s'assurer que tous les membres du personnel ayant accès au système d'information détiennent les attestations de sécurité requises et appropriées;

La classe technique est composée des familles suivantes :

a. **Identification et authentification (IA)** – contrôles de sécurité qui servent à l'identification unique des utilisateurs et à leur authentification lorsqu'ils tentent d'accéder au système d'information;

b. **Contrôle d'accès (CA)** – contrôles de sécurité qui permettent de donner ou de refuser l'accès d'un utilisateur aux ressources contenues dans un système d'information;

c. **Vérification et responsabilité (VR)** – contrôles de sécurité qui permettent de recueillir, d'analyser et de stocker des rapports de vérification liés aux interventions de l'utilisateur dans le système d'information;

d. **Protection du système et des communications (SC)** – contrôles de sécurité qui garantissent la protection du système d'information en soi ainsi que de toutes communications internes et externes du système d'information.

Annexe A : Acronymes et abréviations

Acronyme/ Abréviation	Nom complet
ASE	Agent de sécurité d'entreprise
ASEI	Agent de sécurité d'entreprise intérimaire
ASO	Agent de sécurité organisationnel
CA	Contrôle d'accès
CISR	Commission de l'immigration et du statut de réfugié du Canada
CSTC	Centre de la sécurité des télécommunications Canada
CSTI	Coordonnateur de la sécurité de la technologie de l'information
DP	Demande de propositions
DSIC	Direction de la sécurité industrielle canadienne
GC	Gouvernement du Canada
GRC	Gendarmerie royale du Canada
GSTI	Gestion de la sécurité de la technologie de l'information
IA	Identification et authentification
ITSG	Conseils en matière de sécurité de la technologie de l'information
PS	Protection des supports
PSG	Politique sur la sécurité du gouvernement
RI	Réaction aux incidents
SC	Protection du système et des communications
SCT	Secrétariat du Conseil du Trésor
SF	Sensibilisation et formation
SP	Sécurité du personnel
STI	Sécurité de la technologie de l'information
TED	Traitement électronique des données
TI	Technologie de l'information
TPSGC	Travaux publics et Services gouvernementaux Canada
VOD	Vérification d'organisation désignée
VR	Vérification et responsabilité

Annexe B : Contrôles de sécurité sur mesure

***Nota* :** Comme le choix des contrôles de sécurité peut être subjectif, des efforts considérables ont été déployés en vue d'inclure seulement les contrôles de sécurité qui atténuent les menaces réelles en matière de divulgation et de perte de confidentialité relativement aux renseignements de nature particulièrement délicate désignés Protégé B et qui peuvent être appliqués au moyen de produits disponibles sur le marché et facilement accessibles. Les contrôles de sécurité qui nécessitent une capacité spécialisée ou avancée et non essentielle à un système d'information ont été exclus des contrôles de sécurité sur mesure. Tout a été mis en œuvre pour arriver à un bon équilibre entre la facilité d'utilisation, la sécurité et la rentabilité.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
Contrôles de sécurité opérationnels			
Sensibilisation et formation (SF)			
SF-2	Formation en matière de sécurité	L'organisation fournit une formation liée à la sécurité à tous les utilisateurs avant de leur autoriser l'accès au système ou avant qu'ils n'exécutent des fonctions qui leur ont été assignées.	L'organisation doit déterminer le contenu approprié de la formation en matière de sécurité en fonction du matériel fourni à l'ASE par la CISR.
Réaction aux incidents (RI)			
RI-1	Procédure de réaction aux incidents	A) L'organisation élabore, diffuse et examine ou met à jour une procédure documentée afin de faciliter la mise en œuvre d'une réaction aux incidents en ce qui concerne les incidents de sécurité. La procédure de réaction aux incidents : a) fournit à l'organisation une approche de haut niveau pour ce qui est de mettre en œuvre sa capacité de réaction aux incidents; b) décrit la structure et l'organisation de la capacité de réaction aux incidents; c) définit les incidents à signaler; d) est examinée et approuvée par des agents désignés au sein de l'organisation. B) l'organisation distribue des copies du plan de réaction aux incidents à tous les utilisateurs d'un système d'information. C) l'organisation examine et met à jour, au besoin, la procédure de réaction aux incidents au moins tous les trois (3) ans.	Il est important que les organisations aient une approche officielle, ciblée et coordonnée en ce qui concerne la réaction aux incidents.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
RI-2	Formation en matière de réaction aux incidents	L'organisation forme le personnel en ce qui a trait à ses rôles et responsabilités en cas de réaction aux incidents concernant le système d'information dans le cadre de la formation en matière de sécurité (se reporter au contrôle SF-2).	
RI-4	Traitement des incidents	L'organisation met en œuvre une capacité de traitement des incidents pour les incidents de sécurité qui comprend la préparation, la détection et l'analyse, le confinement, l'éradication et la reprise.	Tous les incidents de sécurité devraient être portés à l'attention de l'ASE dès qu'ils surviennent ou qu'ils sont détectés par tout employé ou entrepreneur organisationnel.
RI-5	Surveillance des incidents	L'organisation surveille et documente les incidents de sécurité touchant les systèmes d'information.	La documentation des incidents de sécurité touchant les systèmes d'information comprend notamment la tenue des dossiers concernant chaque incident, l'état de l'incident et d'autres renseignements pertinents nécessaires à l'égard de l'investigation et de l'évaluation des détails, des tendances et du traitement relatifs à l'incident. Les renseignements sur les incidents peuvent être obtenus d'une diversité de sources, y compris les rapports d'incident, les équipes de réaction aux incidents, le contrôle de la vérification, le contrôle de réseaux, le contrôle et l'accès physique et les rapports de l'utilisateur ou de l'administrateur.
RI-6	Signalement des incidents	A) L'organisation exige que le personnel signale les incidents de sécurité suspects à l'ASE. B) L'organisation signale tous les renseignements sur les incidents de sécurité à l'ASE dans les vingt-quatre (24) heures. C) L'ASE mène une investigation concernant chaque incident de sécurité. Tous les rapports d'incident de sécurité doivent être soumis à l'ASO de la CISR dans les soixante-douze (72) heures suivant le signalement de l'incident à l'ASE.	Ce contrôle vise à respecter les exigences particulières relatives au signalement des incidents au sein de l'organisation de l'entrepreneur et les exigences officielles relatives au signalement des incidents pour la CISR. Les types d'incidents de sécurité signalés, le contenu des rapports et la rapidité de production des rapports et la liste des autorités désignées pour le signalement d'un incident doivent être conformes aux lois du GC et aux politiques, aux directives et aux normes du SCT applicables.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
PS-1	Protection des supports	L'organisation limite l'accès aux supports numériques qui servent au stockage des renseignements de nature délicate aux utilisateurs autorisés. Les supports numériques comprennent notamment les disques durs externes ou amovibles, les disques à mémoire flash ou les clés de stockage, les disques compacts et les disques vidéo numériques.	Les appareils d'informatique mobile et de communications qui ont une capacité d'enregistrement (p. ex. assistants numériques, téléphones cellulaires, téléphones intelligents et appareils-photos numériques) ne devraient pas être utilisés avec un système d'information qui détient des renseignements de nature délicate de la CISR désignés Protégé B.
PS-2	Accès aux supports	Le système d'information utilise des mécanismes de chiffrement cryptographique pour protéger et limiter l'accès à l'information désignée Protégé B qui est stockée sur des supports numériques portables (p. ex. clés USB, disques à mémoire flash ou clés de stockage).	
PS-3	Marquage des supports	L'organisation marque, conformément aux normes gouvernementales, tous les supports amovibles du système d'information et les données de sortie du système d'information qui indiquent les limites de la distribution, les oppositions relatives au traitement et les marquages de sécurité applicables (le cas échéant) de l'information. Reportez-vous aux Normes de sécurité relatives à l'organisation et l'administration du SCT pour obtenir une orientation à cet égard.	

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
PS-4	Stockage des supports	A) L'organisation contrôle physiquement et stocke de façon sécurisée tous les supports numériques au sein des zones de travail contrôlées qui ont été définies par l'organisation, conformément au Guide d'équipement de sécurité (G1-001) de la GRC. B) L'organisation protège physiquement et stocke de façon sécurisée les supports du système d'information désignés Protégé B en attente d'élimination (sur place ou à l'extérieur) en utilisant les techniques, les procédures et le matériel approuvés par le gouvernement.	
PS-5	Transport des supports	A) L'organisation protège et contrôle les supports numériques au cours du transport à l'extérieur des zones contrôlées conformément à la Norme opérationnelle sur la sécurité matérielle du SCT et le guide de sécurité matérielle Transport et transmission de renseignements protégés ou classifiés (G1-009) de la GRC. B) L'organisation demeure responsable des supports du système d'information au cours du transport à l'extérieur des zones contrôlées. C) L'organisation limite les activités associées au transport de tels supports au personnel autorisé. D) L'organisation documente les activités associées au transport des supports du système d'information. E) L'organisation emploie un gardien désigné tout au long du transport des supports du système d'information.	

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
PS-6	Nettoyage des supports	L'organisation nettoie les supports du système d'information, numériques ou non, avant l'élimination, la diffusion hors du contrôle organisationnel ou la diffusion en vue d'une réutilisation.	Ce contrôle s'applique à tous les supports assujettis à une élimination ou à une réutilisation, qu'ils soient considérés ou non comme amovibles. Le nettoyage est le processus utilisé pour retirer de l'information des supports du système d'information, de sorte qu'il y ait une assurance raisonnable que l'information ne peut être récupérée ou reconstituée. Les techniques de nettoyage, y compris l'écrasement, l'expurgation et la destruction de l'information relative aux supports, empêchent la divulgation des renseignements de nature délicate aux personnes non autorisées quand de tels supports sont réutilisés ou envoyés en vue d'être éliminés.
SP-6	Ententes relatives à l'accès	L'organisation veille à ce que les personnes qui peuvent avoir accès aux systèmes d'information et aux renseignements de nature délicate de la CISR signent les ententes relatives à l'accès appropriées avant de se voir accorder l'accès.	Les ententes relatives à l'accès comprennent, par exemple, les ententes de non-divulgation, les ententes d'utilisation acceptable et les règles de conduite. Les ententes relatives à l'accès signées comprennent une reconnaissance que les personnes ont lu, comprennent et acceptent de respecter les contraintes liées au système d'information et aux renseignements auxquels l'accès est autorisé.
Contrôles de sécurité techniques			
Identification et authentification (IA)			
IA-2	Identification et authentification (utilisateurs organisationnels)	A) Le système d'information identifie et authentifie uniquement les utilisateurs organisationnels. Ceux-ci comprennent les employés organisationnels ou les personnes de l'organisation dont on a jugé qu'elles possédaient un statut équivalent à celui d'employé (p. ex., entrepreneurs). B) Les utilisateurs doivent être identifiés et authentifiés de façon unique pour tous les accès à un système d'information.	L'authentification de l'identité des utilisateurs peut se réaliser par l'utilisation de mots de passe, de certificats, de jetons, de renseignements biométriques ou, dans le cas d'une authentification multifactorielle, d'une combinaison des éléments mentionnés.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
IA-4	Gestion des identificateurs	A) L'organisation gère les identificateurs du système d'information pour les utilisateurs (p. ex. identificateur d'utilisateur) en recevant l'autorisation d'un agent organisationnel désigné concernant la désignation d'un identificateur d'utilisateur. B) L'organisation sélectionne un identificateur qui identifie uniquement une personne. C) L'organisation désactive l'identificateur d'utilisateur après cent quatre-vingts (180) jours d'inactivité.	

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
IA-5	Gestion des authentificateurs	A) L'organisation gère les authentificateurs du système d'information pour les utilisateurs en vérifiant, dans le cadre de la distribution initiale des authentificateurs, l'identité de la personne qui reçoit l'authentificateur. B) L'organisation gère les authentificateurs du système d'information pour les utilisateurs en établissant et en mettant en œuvre des procédures administratives pour la distribution initiale des authentificateurs, pour les authentificateurs perdus ou compromis et pour les authentificateurs révoqués. C) L'organisation change le contenu par défaut des authentificateurs dès l'installation du système d'information (c.-à-d., qu'elle n'utilise pas les authentificateurs par défaut). D) L'organisation établit des restrictions de durée minimale et maximale et des conditions de réutilisation pour les authentificateurs. E) L'organisation change ou rafraîchit les authentificateurs au moins une fois par année. F) L'organisation protège le contenu des authentificateurs de la divulgation et de la modification non autorisées.	Les authentificateurs de l'utilisateur comprennent, par exemple, les mots de passe, les jetons, les renseignements biométriques, les certificats et les cartes-clés. Le contenu initial des authentificateurs est le contenu réel (p. ex. le mot de passe initial) plutôt que les exigences concernant le contenu des authentificateurs (p. ex. longueur minimale du mot de passe). Bon nombre de composantes du système d'information sont envoyées avec des légitimations d'authentification réglées par défaut afin de permettre l'installation et la configuration initiales. Les légitimations d'authentification par défaut sont souvent bien connues, faciles à découvrir et présentent un risque important en matière de sécurité; par conséquent, elles doivent être changées au moment de l'installation.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
IA-5	Gestion des authentificateurs	Pour l'authentification qui repose sur un mot de passe, le système d'information doit : a) se conformer à la Politique sur les mots de passe de la CISR; b) appliquer une exigence minimale en ce qui concerne la complexité des mots de passe, conformément à l'Annexe A – Normes de création des mots de passe de la Politique sur les mots de passe de la CISR; c) chiffrer tous les mots de passe en mémoire et en cours de transmission.	
IA-6	Rétroaction des authentificateurs	A) Le système d'information occulte la rétroaction de l'information d'authentification au cours d'un processus d'authentification pour protéger l'information contre toute exploitation ou utilisation possible par des personnes non autorisées.	La rétroaction du système d'information ne fournit pas d'information qui permettrait à un utilisateur non autorisé de compromettre le mécanisme d'authentification. L'affichage d'astérisques quand un utilisateur inscrit un mot de passe est un exemple d'occultation de la rétroaction de l'information d'authentification.
Contrôle d'accès (CA)			

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
CA-2	Gestion des comptes	A) L'organisation gère les comptes du système d'information, y compris l'identification des types de comptes (p. ex. individuel, de groupe, du système, de l'application, invité ou anonyme et temporaire). B) L'organisation identifie les utilisateurs autorisés du système d'information et précise leurs privilèges en matière de contrôle d'accès. C) L'organisation gère un processus approprié d'approbation en ce qui concerne les demandes afin d'établir des comptes d'utilisateur. D) L'organisation crée, active, modifie, désactive et supprime des comptes d'utilisateur. E) L'organisation avise les gestionnaires responsables en cas de changements : lorsque les utilisateurs sont mis à pied ou mutés ou qu'ils ont besoin d'accéder au système. F) L'organisation désactive les comptes d'utilisateur mis à pied ou mutés. G) L'organisation gère les examens de tous les comptes pour ce qui est du besoin d'accéder en continu au moins une fois l'an.	
CA-7	Tentatives de connexion infructueuses	A) Le système d'information applique une limite de cinq (5) tentatives de connexion invalides consécutives par un utilisateur. B) Le système d'information verrouille automatiquement le compte jusqu'à ce que le verrou soit débloqué par un administrateur.	

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
CA-8	Notification de l'utilisation du système	A) Le système d'information affiche un message ou un énoncé approuvé de notification de l'utilisation du système avant de donner l'accès au système; ce message ou cet énoncé fournit des avis en matière de protection des renseignements personnels et de sécurité conformément à la Politique d'utilisation des réseaux électroniques du SCT. B) Le système d'information conserve le message ou l'énoncé de notification à l'écran jusqu'à ce que les utilisateurs prennent des mesures concrètes (p. ex. cliquent sur un bouton <accepter>) pour entrer dans le système d'information.	
CA-17	Accès à distance	**L'accès à distance n'est pas autorisé dans le cas d'un système d'information qui renferme des renseignements de nature délicate de la CISR.**	L'accès à distance correspond à tout accès à un système d'information par un utilisateur qui communique au moyen d'un réseau externe (p. ex. Internet, réseau sans fil, réseau cellulaire). L'accès à un système d'information organisationnel peut être local ou en réseau. L'accès local s'entend de tout accès à un système d'information organisationnel par un utilisateur où l'accès est obtenu grâce à une connexion directe sans l'utilisation d'un réseau. L'accès en réseau s'entend de tout accès à un système d'information organisationnel par un utilisateur où l'accès est obtenu grâce à une connexion au réseau. L'accès en réseau ne sera autorisé que sur les réseaux locaux qui sont logiquement et physiquement isolés de tous les autres réseaux internes et externes utilisés par l'organisation.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
CA-18	Accès sans fil	**L'accès à distance n'est pas autorisé dans le cas d'un système d'information qui renferme des renseignements de nature délicate de la CISR.**	Les technologies sans fil comprennent, mais sans s'y limiter, les hyperfréquences, les satellites, la radiocommunication à commutation de paquets (UHF/VHF), la norme 802.11 et le standard Bluetooth. Dans certaines situations, les signaux sans fil peuvent rayonner au-delà des limites et de la portée des installations contrôlées par l'organisation.
CA-19	Contrôle d'accès pour les appareils mobiles	**L'accès à distance n'est pas autorisé dans le cas d'un système d'information qui renferme des renseignements de nature délicate de la CISR.**	Les appareils mobiles comprennent les appareils informatiques et les appareils de communications portables qui ont une capacité d'enregistrement (p. ex. assistants numériques, téléphones cellulaires et téléphones intelligents qui communiquent dans un réseau cellulaire ou Internet).
Vérification et responsabilisation (VR)			
VR-2	Événements vérifiables	Le système d'information vérifie dans une certaine mesure les événements touchant les utilisateurs et les processus suivants : a) les tentatives de connexion des utilisateurs réussies et infructueuses; b) l'heure de début et de fin de l'accès des utilisateurs au système; c) toutes les mises en marche des programmes.	

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
VR-3	Contenu des registres de vérification	Le système d'information produit des registres de vérification qui contiennent suffisamment d'information pour, à tout le moins, établir le type d'événement qui a eu lieu, le moment (la date et l'heure) où l'événement a eu lieu, le lieu où l'événement s'est produit, la source de l'événement, le résultat (réussite ou échec) de l'événement et l'identité de tout utilisateur associé à l'événement.	
VR-6	Examen, analyse et rapports de vérification	L'organisation examine et analyse les registres de vérification du système d'information au moins une fois par semaine pour y trouver des indications relatives à des activités inappropriées ou inhabituelles et signale ses conclusions à l'ASE.	
VR-8	Horodateurs	Le système d'information utilise des horloges de système fiables permettant de générer des horodateurs (date et heure) pour les registres de vérification.	Les horloges peuvent être synchronisées de façon automatique avec une source fiable pour ce qui est de l'heure par l'intermédiaire d'un protocole de synchronisation réseau (NTP), ou l'organisation peut mettre en œuvre une procédure manuelle pour veiller à ce que la date et l'heure correctes figurent sur tous les ordinateurs hébergeant un système d'information.
Protection du système et des communications			

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
SC-7	Protection des limites	A) Le système d'information ne doit pas se connecter à des réseaux externes (p. ex. d'autres réseaux locaux organisationnels, des réseaux étendus et Internet). B) L'organisation limite le nombre de points d'accès au système d'information pour permettre la surveillance du trafic sur le réseau. C) L'organisation assure une protection et une surveillance de façon à se prémunir contre les connexions physiques non autorisées par-delà les protections des limites.	Les appareils de protection des limites comprennent notamment les serveurs mandataires, les passerelles, les routeurs, les pare-feu et les gardiens.
SC-9	Confidentialité et intégrité de la transmission	Le système d'information protège la confidentialité et l'intégrité de l'information transmise dans l'ensemble des réseaux internes.	
SC-13	Utilisation de la cryptographie	Au besoin, le système d'information implante des protections cryptographiques au moyen de systèmes cryptographiques qui respectent les lois du GC et les politiques, les directives et les normes du SCT applicables.	Le contrôle de base exige l'utilisation d'algorithmes cryptographiques approuvés par le CSTC, qui comprennent, outre les algorithmes, des longueurs de clé, des cryptopériodes, des modes opératoires, des protocoles de bourrage et la génération de bits approuvés, qui sont décrits dans l'alerte ITSA-11E, Algorithmes cryptographiques approuvés par le CSTC pour la protection des renseignements sensibles et pour les applications d'authentification et d'autorisation électroniques au sein du gouvernement du Canada.

Identification de contrôle	Nom	Définition	Renseignements supplémentaires
SC-28	Protection de l'information inactive	Le système d'information protège la confidentialité et l'intégrité de l'information inactive.	Ce contrôle vise à assurer la confidentialité et l'intégrité de l'information inactive dans les appareils non mobiles et comprend l'information relative aux utilisateurs, aux systèmes et aux bases de données. Information inactive s'entend de l'état de l'information au moment où elle est localisée sur une mémoire secondaire (p. ex. disque dur, dérouleur de bande). Les configurations et les séries de règles pour les routeurs, les interrupteurs, les pare-feu et le contenu des authentificateurs sont des exemples d'information du système qui exige une protection. Les organisations peuvent choisir d'employer des mécanismes différents pour assurer une protection de la confidentialité et de l'intégrité, au besoin.