ANNEXE 2, version 2.0

SÉCURITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

Table des matières

1. SÉCURITÉ ET PROTECTION DES RENSEIGNEMENTS PERSONNELS

La présente annexe contient les exigences relatives à la sécurité concernant la solution d'achats électroniques (SAE). À la suite de l'attribution du contrat, le processus d'évaluation et d'autorisation de sécurité de Services publics et Approvisionnement Canada (SPAC), décrit dans la section 6.6, *Processus d'évaluation et d'autorisation de sécurité de TPSGC*, de l'Annexe 1 – Énoncé des travaux, permettra de déterminer la mesure dans laquelle l'entrepreneur respecte ces exigences en vue d'évaluer la conformité aux exigences du Canada en matière de sécurité.

Le gouvernement du Canada a ciblé des contrôles de sécurité afin d'assurer le respect du profil de sécurité des technologies de l'information (TI). La mise en œuvre de cet ensemble de contrôles par l'entrepreneur permettra de s'assurer que les renseignements du gouvernement du Canada dans la SAE sont protégés de façon adéquate pour maintenir un niveau de risque résiduel acceptable pour le Canada. Certains des contrôles de sécurité indiqués dans la section I ci-dessous peuvent être mis à profit au moyen des normes, des attestations et des pratiques exemplaires existantes de l'industrie.

Dans le cadre du processus d'évaluation et d'autorisation de sécurité, si les exigences relatives à la sécurité ne sont pas respectées, le Canada exigera la prise de mesures correctives adéquates pour répondre aux préoccupations soulevées. Le Canada peut, à son entière discrétion, déterminer s'il est convaincu que les mesures correctives sont adéquates.

1.1 MESURE(S) CORRECTIVE(S)

Les contrôles évalués comme non conformes pendant le processus d'évaluation et d'autorisation de sécurité feront l'objet d'une évaluation du Canada relativement à l'exposition aux risques pour les renseignements du gouvernement. Pour les éléments de risque jugés inacceptables par le Canada à la suite du processus d'évaluation et d'autorisation de sécurité, l'entrepreneur doit mettre en œuvre des mesures correctives adéquates pour atténuer les risques associés à la SAE.

1.2 APERÇU

Le présent document compte deux sections :

1. La section I est une liste des exigences relatives à la sécurité qui ont été classées par famille de contrôle dans le document de conseils en matière de sécurité des TI (ITSG) ITSG-33 du Centre de la sécurité des télécommunications Canada (CSTC) [de plus amples renseignements sur le document ITSG-33 se trouvent à l'adresse https://www.cse-cst.gc.ca/fr/node/265/html/22814] ainsi que des pratiques exemplaires du Ministère et de l'industrie. Tout au long de la durée de vie de la SAE, le respect des exigences sera évalué dans le cadre du processus d'évaluation et d'autorisation de sécurité.

2. La section II est un exemple de la matrice de traçabilité des exigences relatives à la sécurité.

1.3 SAE – SÉCURITÉ DE LA TI POUR LE MODÈLE « LOGICIEL COMME SERVICE »

Le gouvernement du Canada va de l'avant pour s'harmoniser avec l'industrie en adoptant des normes et des pratiques exemplaires relatives à l'échange de renseignements. Pour faciliter la réalisation de cette initiative, le CSTC a élaboré le document *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* (méthode présentée dans le document ITSG-33 du CSTC), qui fournit les outils et l'orientation nécessaires aux organisations du gouvernement du Canada et aux entrepreneurs qui travaillent au nom de celui-ci pour s'assurer que les risques liés aux systèmes d'information du gouvernement du Canada sont :

- déterminés;
- signalés;
- atténués tout au long du cycle de vie du système.

Pendant toute la durée du contrat, le besoin de protéger les renseignements du gouvernement du Canada est de la plus grande importance et constitue la force motrice nécessaire pour déterminer la meilleure méthode de protection des ressources d'information.

Les besoins opérationnels en matière de sécurité définissent les objectifs opérationnels en matière de sécurité, qui sont utilisés pour sélectionner les contrôles applicables dans le catalogue des contrôles du document ITSG-33 du CTSC en fonction de la nature délicate, de l'intégrité et de la disponibilité des renseignements.

1.4 POINTS DE CONTRÔLE DU PROCESSUS D'ÉVALUATION ET D'AUTORISATION DE SÉCURITÉ

Le processus d'évaluation et d'autorisation de sécurité est fondé sur le cycle de développement de systèmes. Pour la SAE, le gouvernement du Canada a établi trois points de contrôle dans le processus d'évaluation et d'autorisation de sécurité, afin de s'assurer que la SAE est conçue, développée et intégrée en y incorporant les mesures de sécurité, pour ainsi favoriser la sécurité et la stabilité de la Solution pour le gouvernement du Canada. Il s'agit d'une approche itérative à la migration de la SAE à partir de l'environnement de conception et développement vers à l'environnement opérationnel. Le gouvernement du Canada a établi un ensemble de produits livrables attendus à chaque point de contrôle. La conformité de ces produits livrables sera examinée et évaluée, par le gouvernement du Canada, par rapport aux exigences figurant à la *section I* de la présente annexe. En outre, considérant que certains domaines du modèle SaaS puissent ne pas être visibles par le gouvernement du Canada, l'entrepreneur doit soumettre à l'examen du gouvernement du Canada tous les accords sur les niveaux de service et tous les protocoles d'entente qui sont en place afin de faciliter la compréhension de la posture de sécurité de la SAE.

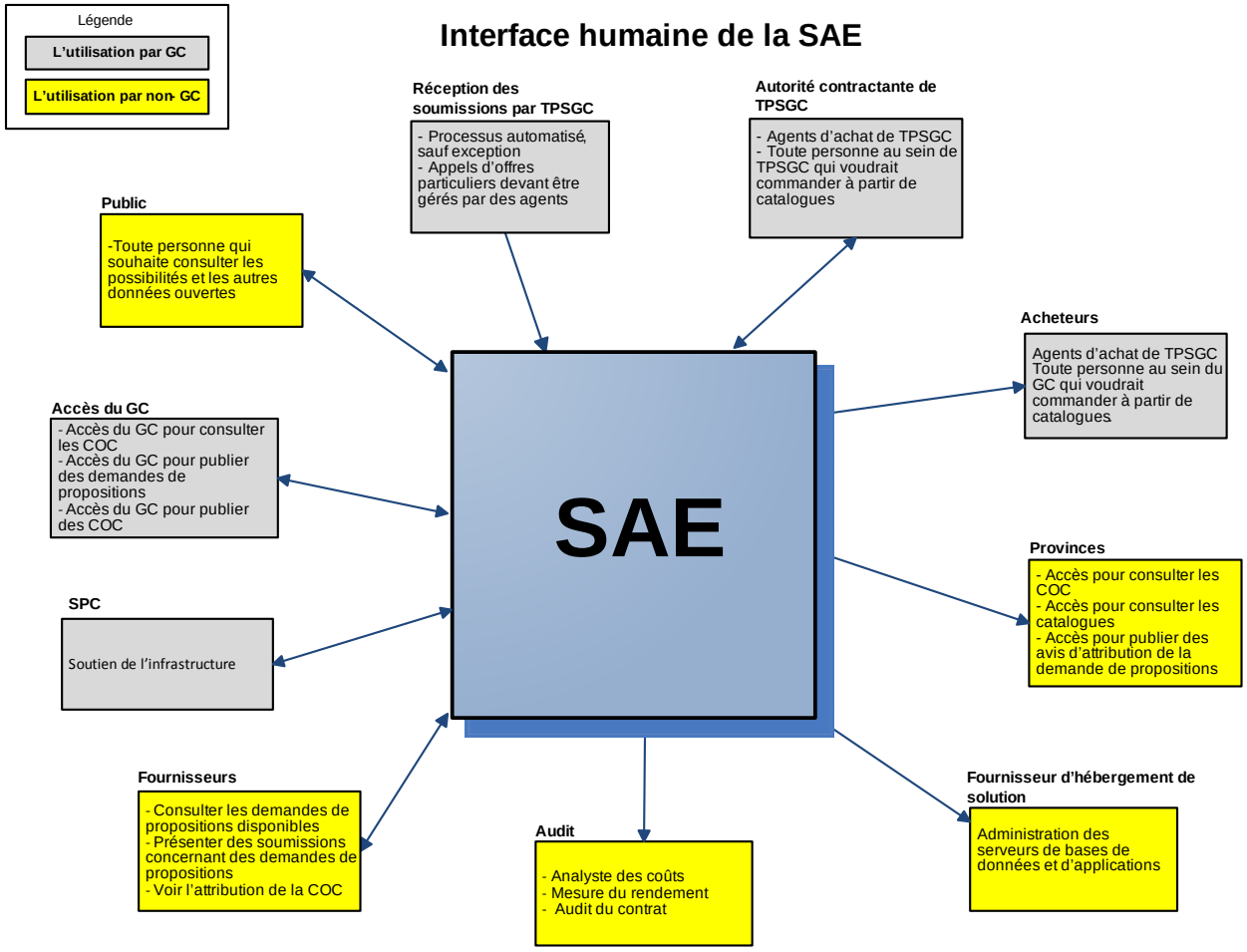
L'entrepreneur doit préciser les normes et les attestations de l'industrie auxquelles il se conforme à l'appui de la SAE qu'il propose. L'une de ces normes, SAS 70 comprend des procédures d'exploitation relatives à la sécurité physique et à la sécurité du périmètre des centres de données et des fournisseurs de services. L'accès à des données de nature délicate de même que le stockage et le traitement de ces données doivent être contrôlés attentivement, et ils sont régis par des normes, comme la norme ISO-27001, la loi Sarbanes-Oxley, la loi Gramm-Leach-Bliley, la *Health Insurance Portability and Accountability*

Act et des normes de l'industrie, comme la Norme de sécurité des données de l'industrie des cartes de paiement.

1.5 CONTEXTE OPÉRATIONNEL

1.5.1 Cas d'utilisation opérationnelle

La **Figure 1** ci-dessous donne un aperçu des cas d'utilisation opérationnelle des interfaces humaines associées à la SAE. Elle illustre la diversité de la base d'utilisateurs de la SAE.



1.6 RÉSUMÉ DU CONTEXTE TECHNIQUE

La SAE doit être un logiciel-service sous une plateforme Web (SaaS) offrant des services communs d'approvisionnement pour le gouvernement du Canada, disponible de l'intérieur et de l'extérieur de l'environnement du gouvernement du Canada celui-ci. Les exigences technologiques de la SAE sont définies dans la section 4.4, Exigences technologiques de la SAE de l'Annexe 1 – Énoncé des travaux.

Bien que la SAE doive être hébergée comme une solution informatique en nuage, l'entrepreneur doit assurer la séparation des données du gouvernement du Canada. La SAE doit également procéder à un

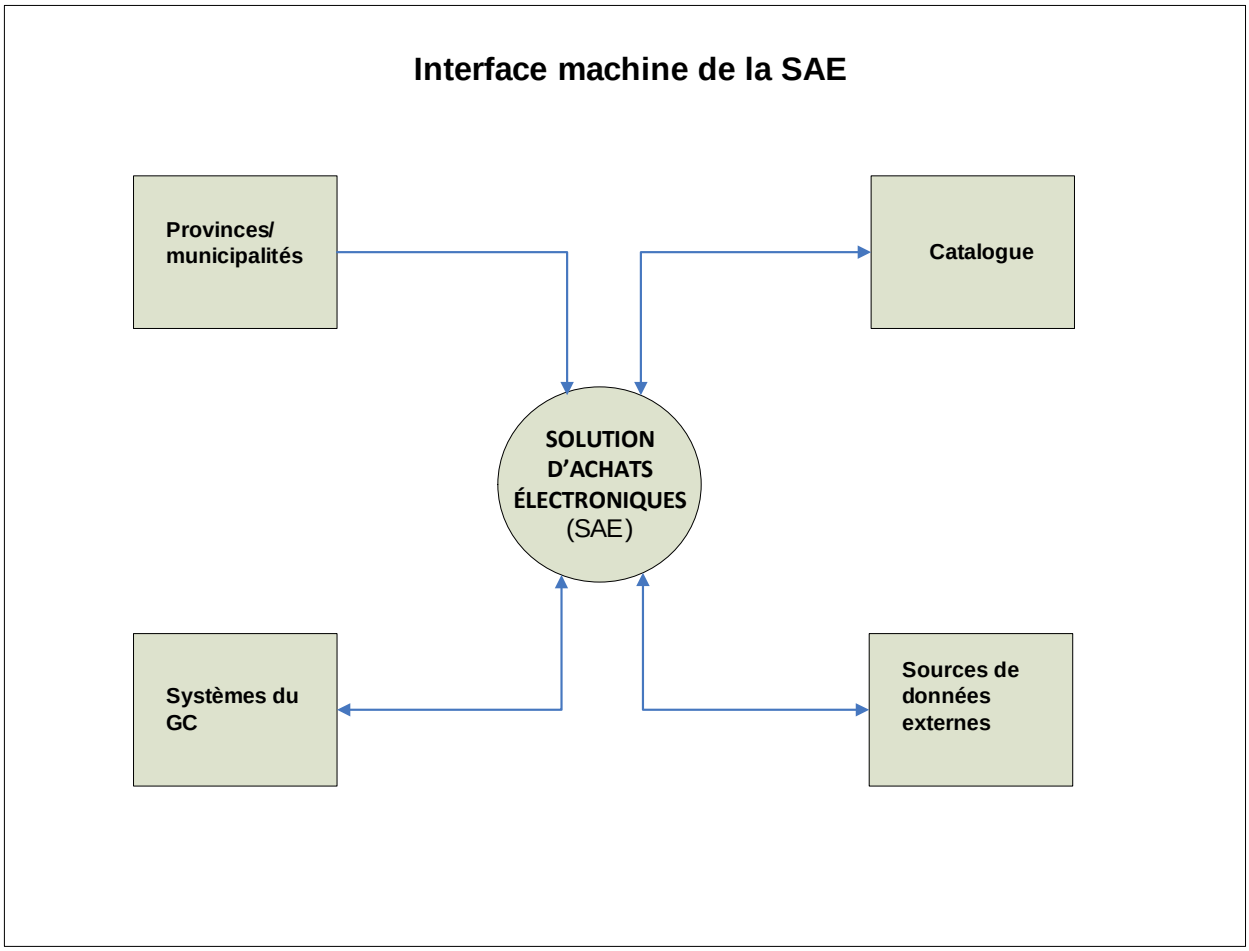
échange sécurisé des données avec les autres systèmes de soutien (à l'intérieur comme à l'extérieur du gouvernement) et les systèmes administratifs en place, ainsi qu'avec ceux qui seront mis en place dans un proche avenir. Par exemple, la SAE devrait jouer un rôle clé dans le processus d'achat au paiement du gouvernement du Canada. Bien que ce processus soit encore à l'étape de la planification, la SAE doit faire partie intégrante du processus opérationnel global visant à le prendre en charge.

La SAE doit communiquer, par l'intermédiaire de l'Enterprise Service Bus (EBS), avec les multiples occurrences (versions) opérationnelles de SAP, le système ministériel de gestion des finances et du matériel. Le principal outil d'interopérabilité entre les processus opérationnels et les systèmes administratifs du gouvernement du Canada est le bus de service l'ESB d'Oracle. L'ESB est en cours d'élaboration pour le gouvernement du Canada et devrait être mis en application à temps pour la mise en œuvre de la SAE. Pour en savoir plus sur les exigences d'interopérabilité de la SAE, consulter la section 4.3, Interfaces avec les systèmes gouvernementaux, de l'Annexe 1 – Énoncé des travaux.

La SAE doit permettre l'ouverture d'une session sécurisée par l'intermédiaire des services de gestion de l'identité, des justificatifs d'identité et de l'authentification (GIJIA) approuvés par le gouvernement du Canada, en plus d'un contrôle d'accès sécurisé aux diverses composantes du système. Pour en savoir plus sur les exigences en matière d'accès sécurisé, consulter la section 4.5, Accès sécurisé, de l'Annexe 1 – Énoncé des travaux.

1.6.1 Interface machine

La **Figure 2** ci-dessous donne un aperçu de l'interface machine associée à la SAE.



1.7 DESCRIPTION DES CLASSES ET DES FAMILLES DE CONTRÔLE DES POLITIQUES ET DES PROCÉDURES DE SÉCURITÉ

Voici une description très générale du catalogue des contrôles de sécurité (ITSG-33) divisé en classes et en familles de contrôle. Ces familles de contrôle s'appliquent aux exigences de sécurité de la SAE. Elles sont présentées selon les exigences énumérées dans la présente annexe. Elles sont le fondement de la sécurité de l'application (logiciel) et des données.

1.7.1 La classe de contrôles de sécurité techniques comprend les familles de contrôle suivantes :

Contrôle d'accès : Contrôles de sécurité permettant d'autoriser ou d'interdire l'accès à un utilisateur aux ressources contenues dans un système d'information.

Vérification et responsabilité : Contrôles de sécurité permettant de recueillir, d'analyser et de stocker des rapports de vérification liés aux interventions de l'utilisateur dans le système d'information.

Identification et authentification : Contrôles de sécurité permettant de vérifier l'identification et l'authentification uniques des utilisateurs lorsqu'ils tentent d'accéder aux ressources du système d'information.

Protection du système et des communications : Contrôles de sécurité permettant de protéger le système d'information ainsi que ses communications internes et externes.

1.7.2 La classe de contrôles de sécurité opérationnels comprend les familles de contrôle suivantes :

Sensibilisation et formation : Contrôles de sécurité qui se rapportent à la formation des utilisateurs quant à la sécurité du système d'information.

Gestion de la configuration : Contrôles de sécurité facilitant la gestion et l'administration de tous les composants du système d'information (p. ex. matériel, logiciel et éléments de configuration).

Planification d'urgence : Contrôles de sécurité permettant l'accès aux services du système d'information en cas de défaillance d'un composant ou de sinistre.

Intervention en cas d'incident : Contrôles de sécurité permettant de détecter, d'intervenir et de signaler les incidents de sécurité liés au système d'information.

Maintenance : Contrôles de sécurité facilitant la maintenance du système d'information pour assurer sa disponibilité à long terme.

Protection des supports : Contrôles de sécurité permettant de protéger les supports du système d'information (disques, bandes magnétiques, etc.) tout au long de leur cycle de vie.

Protection physique et environnementale : Contrôles de sécurité liés à l'accès physique à un système d'information et à la protection de l'équipement environnemental auxiliaire (électricité, climatisation, câblage, etc.) servant à l'exploitation du système d'information.

Sécurité du personnel : Contrôles de sécurité servant à appliquer les procédures nécessaires pour veiller à ce que tous les membres du personnel ayant accès au système d'information détiennent les autorisations de sécurité requises.

Intégrité du système et de l'information : Contrôles de sécurité permettant de protéger l'intégrité des composants du système d'information et des données traitées par ce système.

1.7.3 La classe de contrôles de sécurité de gestion comprend les familles de contrôle suivantes :

Évaluation et autorisation de sécurité : Contrôles de sécurité concernant l'évaluation de sécurité et l'autorisation du système d'information.

Planification : Contrôles de sécurité concernant les activités de planification de la sécurité, y compris l' évaluation des facteurs relatifs à la protection des renseignements personnels.

Évaluation des risques : Contrôles de sécurité concernant l'exécution des évaluations des risques et l'analyse de la vulnérabilité.

Acquisition des systèmes et des services : Contrôles de sécurité concernant la passation de marchés pour l'acquisition de produits et des services nécessaires à la mise en œuvre et à l'exploitation du système d'information.

SECTION I – EXIGENCES RELATIVES À LA SÉCURITÉ

Le tableau 1 ci-dessous décrit en détail les exigences relatives à la SAE.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.1	Contrôle de l'accès	L'entrepreneur doit : a) élaborer, diffuser, examiner, réviser et mettre à jour chaque année les politiques sur le contrôle d'accès et les exigences connexes en matière de contrôle d'accès pour les composantes de la SAE; b) fournir au gouvernement du Canada les procédures de sécurité opérationnelles qui définissent les rôles opérationnels et les responsabilités en matière de contrôle d'accès.
E2.2	Contrôle de l'accès	Les services de GIJIA doivent créer automatiquement des comptes d'utilisateur et des comptes génériques pour la SAE, c'est-à-dire : a) attribuer un compte et un nom d'affichage uniques pour la SAE, conformément à la norme définie dans l'Énoncé des travaux, en appliquant les règles configurables de résolution de conflits et de désignation; b) créer un compte sans privilège; c) attribuer un mot de passe temporaire applicable au compte; d) établir les attributs du compte et les privilèges de sécurité d'accès selon les directives du gouvernement du Canada; e) communiquer le compte, le nom d'affichage et le mot de passe unique attribués pour la SAE au demandeur du compte.
E2.3	Contrôle de l'accès	Les services de GIJIA doivent : a) prévenir la réutilisation d'un compte relatif à la SAE selon les directives du gouvernement du Canada; b) autoriser les politiques de suspension de comptes, selon les directives du gouvernement du Canada; c) interdire l'accès à un compte suspendu; d) s'assurer qu'un compte suspendu n'envoie ni ne reçoit de message lié au déroulement de travaux de la SAE; e) interdire l'accès direct au service de la SAE à partir de tout compte, selon les directives du gouvernement du Canada.
E2.4	Contrôle de l'accès	L'entrepreneur doit gérer les comptes des opérateurs de la SAE : a) en déterminant les types de comptes (c.-à-d. individuel, collectif, relatif à un système, à un appareil ou à une application, invité/anonyme, et temporaire); b) en établissant les conditions pour l'adhésion à des groupes; c) en déterminant les opérateurs autorisés de la SAE et en précisant les droits d'accès; d) en demandant les approbations requises pour les demandes d'établissement de comptes; e) en sélectionnant un identifiant qui identifie uniquement l'opérateur ou l'appareil; f) en attribuant l'identifiant de l'opérateur à la partie visée ou l'identifiant d'appareil à l'appareil visé;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		g) en établissant, en activant, en modifiant, en désactivant et en supprimant les comptes; h) en autorisant et en surveillant précisément l'utilisation des comptes temporaires et des comptes d'invités et anonymes; i) en avisant l'administrateur des comptes lorsqu'un compte temporaire n'est plus requis et lorsque les opérateurs de la SAE quittent leur emploi ou sont mutés, ou lorsque des changements sont apportés à l'utilisation de la SAE ou au principe du besoin de connaître ou au principe du besoin de partager; j) en veillant à ce que les identifiants ne soient pas réutilisés durant au moins un an; k) en désactivant : i) les comptes temporaires qui ne sont plus requis; ii) les comptes des opérateurs qui ont quitté leur emploi ou qui ont été mutés; iii) les comptes après un certain nombre de jours d'inactivité, selon les directives du gouvernement du Canada, iv) les comptes temporaires et les comptes d'urgence après une période donnée; l) en accordant un accès au service de la SAE selon : i) une autorisation d'accès valide, ii) l'utilisation prévue du système; iii) d'autres exigences selon les directives de l'entrepreneur ou du gouvernement du Canada; m) en examinant les comptes au moins une fois par mois; n) en verrouillant les comptes après dix (10) tentatives d'ouverture de session infructueuses dans un délai de cinq (5) minutes; o) en gardant les comptes verrouillés jusqu'à ce qu'ils soient déverrouillés manuellement par un autre opérateur.
E2.5	Contrôle de l'accès	La SAE doit consigner les événements suivants dans un registre : a) création d'un compte; b) modification d'un compte; c) suspension d'un compte; d) clôture d'un compte; e) suppression d'un compte; f) visualisation des comptes de la SAE dont l'utilisateur n'est pas le principal responsable.
E2.6	Contrôle de l'accès	La SAE doit appliquer les autorisations d'accès des opérateurs.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.7	Contrôle de l'accès	La fonction de prévention de pertes de données de la SAE doit : a) détecter les violations des politiques de prévention de pertes de données et appliquer les mesures d'intervention, notamment : i) blocage du transfert de la transaction; ii) blocage du transfert de la transaction et renvoi de la transaction à l'expéditeur; iii) autres mesures convenues par écrit entre l'entrepreneur et le gouvernement du Canada; b) permettre l'application en temps réel des politiques de prévention de pertes de données selon le contenu des attributs des transactions effectués dans la SAE, notamment : i) chaînes, schémas de chaînes, et mots-clés dans le corps de la transaction; ii) type de fichier des pièces jointes; iii) domaines spécifiques, dont ceux comportant souvent du contenu malveillant.
E2.8	Contrôle de l'accès	L'entrepreneur doit veiller à la séparation des tâches des opérateurs, au besoin, afin de prévenir toute activité malveillante et toute collusion en fonction du profil d'accès accordé à l'opérateur selon son rôle.
E2.9	Contrôle de l'accès	L'entrepreneur doit mettre en œuvre la politique du droit d'accès minimal dans l'attribution des privilèges aux opérateurs de la SAE, de la façon suivante : a) configurer les mécanismes de contrôle d'accès de manière à accorder le privilège minimal, soit en donnant uniquement aux opérateurs (et aux processus exécutés en leur nom) l'accès dont ils ont besoin pour accomplir les tâches qui leur sont attribuées; b) créer des comptes non privilégiés qui seront utilisés pour les tâches non opérationnelles; c) limiter l'attribution de comptes super-utilisateur (p. ex. racine) aux opérateurs désignés; d) limiter le partage des comptes des opérateurs; e) identifier de manière unique la personne qui a effectué une tâche dans la SAE.
E2.10	Contrôle de l'accès	La SAE doit : 1. afficher une bannière d'ouverture de session approuvée par le gouvernement du Canada dans la page d'ouverture de session de toute application Web destinée aux utilisateurs; 2. inclure un mécanisme de contrôle de l'accès qui : a) empêche l'accès aux composantes et aux ressources de la SAE sans identification, authentification et autorisation; b) affiche un message d'avertissement pré-approuvé par le gouvernement du Canada lors de l'ouverture de session; l'opérateur autorisé doit accuser réception du message avant d'avoir accès aux composantes de la SAE; c) présente à l'opérateur, lorsqu'il a réussi l'ouverture de session, la date et l'heure d'ouverture de sa session de travail précédente;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		d) offre une fonction de fermeture de session conviviale facile lorsqu'un opérateur a recours à l'authentification pour accéder aux composantes de la SAE; e) inclut un mécanisme de verrouillage de session de l'opérateur qui : i. empêche l'accès à SAE en verrouillant automatiquement la session de l'opérateur après une période d'inactivité de 60 minutes ou plus; ii. empêche tout nouvel accès à SAE en verrouillant automatiquement la session d'un opérateur après une période d'inactivité préconfigurée par l'opérateur; iii. affiche un économiseur d'écran qui ne contient aucune information importante et qui remplace tout le contenu précédemment affiché à l'écran lorsque la session de l'opérateur est verrouillée; iv. déverrouille la session de l'opérateur lorsqu'il réussit à s'authentifier.
E2.11	Contrôle de l'accès	L'entrepreneur doit s'assurer que les opérateurs qui ont recours à la télégestion de la SAE utilisent une méthode approuvée par le Canada qui respecte les conditions suivantes : a) restriction de la télégestion à la SAE située dans un point de prestation de service de l'entrepreneur à l'aide des consoles de gestion prévues de la SAE; b) consignation des méthodes autorisées de gestion à distance, ainsi que des restrictions d'utilisation et des lignes directrices de mise en œuvre pour chacune de ces méthodes; c) détection des cas de gestion à distance non autorisée; d) autorisation de la télégestion avant de permettre la connexion; e) utilisation de mécanismes automatiques pour faciliter la surveillance et le contrôle des méthodes de télégestion; f) acheminement de tous les dossiers de télégestion dans les composantes de la SAE à l'aide d'un nombre limité de points de contrôle d'accès gérés; g) protection de l'information sur les mécanismes de télégestion contre l'utilisation et la divulgation non autorisées; h) utilisation de mécanismes automatiques pour faciliter la surveillance et le contrôle des méthodes de télégestion.
E2.12	Contrôle de l'accès	L'entrepreneur doit établir des politiques et des procédures qui appuient les processus opérationnels et les mesures techniques, mis en œuvre au sein de tout environnement appuyant la SAE afin de protéger celle-ci des environnements de réseau sans fil, notamment : a) les pare-feu du périmètre mis en œuvre et configurés de manière à restreindre le trafic non autorisé; b) les paramètres de sécurité permettant un chiffrement efficace aux fins d'authentification et de transmission, conformément à la norme CST DGSIT-111 visant les données de niveau Protégé B; c) le renforcement de la sécurité en remplaçant les paramètres par défaut du fournisseur (p. ex., clés de cryptage, mots de passe et chaînes de la communauté de protocole de gestion de réseau simple); d) l'accès des utilisateurs, y compris les utilisateurs d'appareils de réseau sans fil, limité au personnel autorisé;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		e) la capacité de détecter la présence d'appareils non autorisés (indésirables) dans le réseau sans fil afin de les débrancher rapidement du réseau.
E2.13	Contrôle de l'accès	L'entrepreneur doit mettre en œuvre une politique sur les appareils mobiles applicable à la SAE; cette politique doit comprendre au minimum ce qui suit : a) formation sur la sensibilisation aux logiciels malveillants propres aux appareils mobiles. Cette formation doit faire partie de la formation sur la sensibilisation à la sécurité de l'information de l'entrepreneur; b) une liste documentée des boutiques d'applications approuvées a été jugée acceptable pour les appareils mobiles qui permettent d'accéder aux données gérées par les fournisseurs et de les stocker; c) l'entrepreneur doit avoir mis en place une politique documentée interdisant l'installation d'applications non approuvées ou d'applications approuvées qui n'ont pas été obtenues auprès d'une boutique d'applications déterminée au préalable; d) le cas échéant, la politique « apportez votre équipement personnel de communication » (AVEC) et la formation de soutien sur la sensibilisation énoncent clairement les applications, les boutiques d'applications et les extensions et modules d'extension des applications approuvés qui peuvent être utilisés dans le cadre de la politique AVEC; e) l'entrepreneur doit disposer d'une politique écrite relativement aux applications mobiles, qui comprend une définition écrite des applications mobiles ainsi que de l'utilisation et des exigences acceptables pour tous les appareils mobiles. Par ailleurs, l'entrepreneur doit publier et communiquer la politique et les exigences en question dans le cadre du programme de sensibilisation et de formation à la sécurité de l'entreprise; f) tous les services infonuagiques utilisés par les appareils mobiles de l'entreprise ou dans le cadre de la politique AVEC doivent être approuvés au préalable pour l'utilisation et le stockage des données opérationnelles liées à la SAE du gouvernement du Canada; g) l'entrepreneur doit avoir mis en place un processus documenté de validation des applications afin de vérifier les problèmes de compatibilité liés aux appareils mobiles, au système d'exploitation et aux applications; h) la politique AVEC doit définir les appareils et les exigences d'admissibilité afin de permettre l'utilisation des appareils aux termes de cette politique; i) l'entrepreneur doit conserver et tenir à jour un répertoire de tous les appareils mobiles utilisés pour stocker les données de la SAE du gouvernement du Canada et y avoir accès; j) l'entrepreneur doit inclure, pour chaque appareil figurant dans le répertoire, des détails sur tous les changements apportés à l'état de ces appareils (c.-à-d. le système d'exploitation et les niveaux de correction, les états des appareils perdus ou mis hors service, les personnes à qui les appareils sont attribués et les appareils approuvés dans le cadre de la politique AVEC); k) une solution centralisée de gestion des appareils mobiles doit être déployée pour tous les appareils mobiles autorisés à stocker, à transmettre ou à traiter les données sur les clients;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		l) la politique sur les appareils mobiles doit exiger l'utilisation du chiffrement pour l'ensemble de l'appareil ou pour les données de nature délicate de tous les appareils mobiles. Elle doit également être renforcée au moyen de contrôles technologiques; m) la politique sur les appareils mobiles doit interdire le contournement des contrôles de sécurité intégrés des appareils mobiles (p. ex. débridage ou racinement) et renforcer l'interdiction au moyen de contrôles de détection et de prévention sur l'appareil ou au moyen d'un système centralisé de gestion des appareils (p. ex. gestion des appareils mobiles) n) la politique AVEC doit, s'il y a lieu, préciser les attentes en matière de protection des renseignements personnels, les exigences en matière de litiges, de découverte électronique et de réserves juridiques. Par ailleurs, la politique AVEC doit clairement énoncer les attentes au sujet de la perte de données opérationnelles non liées à la SAE du gouvernement du Canada s'il faut écraser les données de l'appareil; o) les appareils visés par la politique AVEC et les appareils appartenant à l'entrepreneur sont configurés de manière à nécessiter un écran de verrouillage automatique. Cette exigence doit être appliquée au moyen de contrôles techniques; p) les changements apportés aux systèmes d'exploitation, aux niveaux de correction et aux applications des appareils mobiles doivent être gérés dans le cadre du processus de gestion du changement de l'entrepreneur; q) les politiques relatives aux mots de passe, qui s'appliquent aux appareils mobiles, doivent être documentées et appliquées au moyen de contrôles techniques sur tous les appareils appartenant à l'entrepreneur ou les appareils approuvés aux fins de la politique AVEC. Elles doivent également interdire la modification de la longueur du mot de passe ou du NIP ainsi que des exigences en matière d'authentification; r) la politique sur les appareils mobiles doit exiger aux utilisateurs d'appareils visés par la politique AVEC de faire des copies de sauvegarde des données, interdire l'utilisation de boutiques d'applications non approuvées et exiger l'utilisation de programmes de protection contre les logiciels malveillants (lorsque ces programmes sont supportés); s) tous les appareils mobiles qui peuvent être utilisés dans le cadre du programme AVEC de l'entrepreneur ou les appareils mobiles attribués doivent permettre au responsable ministériel de la TI de l'entrepreneur d'effectuer un nettoyage à distance ou faire en sorte que toutes les données fournies par une entreprise soient nettoyées par le responsable ministériel de la TI de l'entrepreneur; t) les appareils mobiles qui permettent de se connecter aux réseaux de l'entrepreneur ou de stocker des renseignements sur l'entreprise et d'y avoir accès doivent permettre de valider à distance les versions ou les corrections du logiciel; u) tous les appareils mobiles doivent appliquer les plus récents correctifs de sécurité installés lorsque le fabricant ou le transporteur de l'appareil les rend disponibles de façon générale. Le personnel autorisé de la TI doit être en mesure d'appliquer ces mises à jour à distance;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		v) la politique AVEC doit préciser les systèmes et les serveurs qui peuvent être utilisés avec un appareil visé par la politique AVEC ou qui peuvent y accéder.
E2.14	Contrôle de l'accès	SUPPRIMER
E2.15	Contrôle de l'accès	L'entrepreneur doit restreindre l'utilisation des supports de données portatifs (p. ex. clés USB) contrôlés par l'entrepreneur, c'est-à-dire : a) limiter l'utilisation aux opérateurs autorisés seulement; b) limiter l'utilisation aux composantes de la SAE uniquement.
E2.16	Formation et sensibilisation à la sécurité	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité relatives à la SAE qui définissent les rôles et les responsabilités opérationnels en matière de sensibilisation et de formation.
E2.17	Formation et sensibilisation à la sécurité	L'entrepreneur doit tenir des séances de formation et de sensibilisation en matière de sécurité à l'intention des opérateurs de la SAE, comme suit : a) dans le cadre de la formation initiale donnée aux nouveaux opérateurs; b) avant d'accorder un accès à la SAE ou avant l'exécution des tâches attribuées; c) chaque année ou lorsque des changements concernant la sécurité sont apportés à la SAE.
E2.18	Formation et sensibilisation à la sécurité	L'entrepreneur doit surveiller et consigner les séances de sensibilisation et de formation relatives à la sécurité de la SAE données aux opérateurs de la SAE, notamment : a) consigner le nom des participants de chaque cours de formation et la date des cours; b) conserver les documents établis au cours des **trois (3) dernières années**.
E2.19	Vérification et responsabilité	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité relatives à la SAE qui définissent les rôles et les responsabilités opérationnels en matière de vérification et de responsabilité.
E2.20	Vérification et responsabilité	Les services de GIJIA de la SAE doivent consigner les événements suivants selon les exigences en matière de consignation des événements d'authentification pour l'assurance d'authentification de niveau 3, décrites dans le document ITSG-31 (https://www.cse-cst.gc.ca/fr/node/267/html/22784) : a) événements d'authentification réussis; b) événements d'authentification non réussis.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.21	Vérification et responsabilité	L'entrepreneur doit : a) examiner et mettre à jour la liste des événements vérifiables pour la SAE au moins une fois tous les 180 jours ouvrables; b) inclure l'exécution des fonctions privilégiées à la liste des événements de vérification; c) consigner les événements désignés et approuvés par le gouvernement du Canada; d) générer automatiquement des alertes en temps réel (p. ex. à l'aide de règles de corrélation) à la suite d'indications de compromission et de compromission potentielle.
E2.22	Vérification et responsabilité	L'entrepreneur doit s'assurer que la SAE permet d'exécuter les tâches suivantes : a) surveiller les incidents tels que l'accès non autorisé à la SAE, les modifications non autorisées, les modifications apportées aux caractéristiques de sécurité, l'accès privilégié à des champs de données; b) préparer des dossiers de vérification permettant, au minimum, d'établir le type d'événement, la date et l'heure de l'événement, l'endroit où il s'est produit, sa source, son résultat (succès ou échec) ainsi que l'identité de tout utilisateur ou sujet associé à l'événement; classer les événements vérifiés par type, lieu ou sujet, et gérer le contenu des dossiers de vérification générés.
E2.23	Vérification et responsabilité	L'entrepreneur doit assurer la gestion de la capacité de stockage des dossiers de vérification de la SAE en : a) attribuant une capacité de stockage suffisante pour les dossiers de vérification; b) configurant la vérification de manière à empêcher le dépassement de la capacité de stockage; c) alertant le centre des opérations lorsque le volume de stockage des dossiers de vérification atteint 75 % de la capacité de stockage; d) écrasant les dossiers de vérification les plus anciens si la capacité maximale de stockage est atteinte.
E2.24	Vérification et responsabilité	La fonction de vérification de la SAE doit aborder les défaillances en matière de vérification en : a) avisant le centre des opérations; b) écrasant les dossiers de vérification les plus anciens si la capacité maximale est atteinte.
E2.25	Vérification et responsabilité	Afin de générer l'horodatage des dossiers de vérification, la SAE doit régler les horloges internes en synchronisation avec les horloges d'une source faisant autorité et approuvées par le gouvernement du Canada.
E2.26	Vérification et responsabilité	La SAE doit : a) protéger les renseignements de vérification contre l'accès, les modifications et la suppression non autorisés; b) sauvegarder les dossiers de vérification dans un système ou un support différent de celui dont la vérification est prévue au calendrier selon les directives du gouvernement du Canada.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.27	Évaluation et autorisation de sécurité	L'entrepreneur doit élaborer un plan d'atténuation des vulnérabilités de la SAE, aux fins d'approbation par le Canada, dans les cinq (5) jours ouvrables suivant l'achèvement d'une évaluation des vulnérabilités. Le plan doit proposer des mesures de protection pour atténuer les risques décrits dans cette évaluation.
E2.28	Gestion de la configuration	L'entrepreneur doit développer, consigner et gérer la configuration de base courante des composantes de la SAE et des deux (2) versions précédentes.
E2.29	Gestion de la configuration	L'entrepreneur doit permettre uniquement l'exécution des logiciels autorisés, établis par l'entrepreneur et approuvés par le Canada, dans la SAE.
E2.30	Gestion de la configuration	L'entrepreneur doit : a) planifier et mettre à l'essai la mise en œuvre des logiciels, du matériel et des documents nouveaux et modifiés en vue de lancer une version de la SAE sans utiliser l'environnement de production ou l'environnement d'essais contrôlés du service de la SAE; b) mettre en œuvre les logiciels, le matériel et les documents nouveaux et modifiés en vue de lancer une version de la SAE approuvée par le Canada; c) élaborer et mettre en œuvre des procédures de distribution, d'installation et d'annulation des changements apportés en vue du lancement d'une version de la SAE.
E2.31	Gestion de la configuration	L'entrepreneur doit évaluer les répercussions des changements sur la sécurité en : a) analysant les nouveaux logiciels avant de les installer dans un environnement opérationnel, afin d'identifier les répercussions sur la sécurité attribuables à des failles, à des lacunes, à une incompatibilité ou à une malveillance intentionnelle; b) informant le gouvernement du Canada des répercussions possibles sur la sécurité avant de mettre en œuvre des changements; c) vérifiant les fonctions relatives à la sécurité, une fois les changements mis en œuvre, afin de s'assurer que les fonctions s'exécutent correctement, qu'elles fonctionnent comme prévu et qu'elles produisent les résultats escomptés en ce qui a trait aux exigences relatives à la sécurité.
E2.32	Gestion de la configuration	L'entrepreneur doit effectuer des vérifications des changements apportés au système d'information, au moins tous les douze mois et lorsque les circonstances le justifient selon que des changements non autorisés ont été apportés ou non.
E2.33	Gestion de la configuration	L'entrepreneur doit passer en revue les privilèges des opérateurs de la SAE chaque année.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.34	Gestion de la configuration	L'entrepreneur doit utiliser des mécanismes automatisés afin de gérer, d'appliquer et de vérifier les paramètres de configuration de façon centrale et de réagir aux changements non autorisés apportés à la configuration en créant un dossier d'incident de sécurité.
E2.35	Gestion de la configuration	L'entrepreneur doit créer un dossier d'incident de sécurité lorsqu'un changement non autorisé à la configuration est relevé dans la SAE.
E2.36	Gestion de la configuration	L'entrepreneur doit configurer la SAE de manière à fournir uniquement les fonctions essentielles et à interdire ou à restreindre précisément l'utilisation des fonctions, des ports, des protocoles ou des services qui ont été approuvés par le Canada.
E2.37	Gestion de la configuration	L'entrepreneur doit élaborer et tenir un répertoire des composantes de la SAE qui : a) reflète fidèlement la configuration actuelle des composantes; b) respecte le niveau de précision jugé nécessaire au suivi et à l'établissement des rapports; c) comprend les renseignements jugés nécessaires pour exercer une responsabilité efficace à l'égard des biens; d) est accessible aux fins d'examen et de vérification par le gouvernement du Canada; e) est mis à jour en tant que partie intégrante des installations de composantes, des suppressions et des mises à jour de la SAE.
E2.38	Gestion de la configuration	L'entrepreneur doit présenter un plan de gestion de la configuration de la SAE qui : a) décrit les rôles et les responsabilités ainsi que les processus et les procédures de gestion de la configuration; b) définit les éléments de configuration de la SAE et le moment où ces éléments sont soumis au processus de gestion de la configuration; c) définit les moyens de détermination des éléments de configuration tout au long du cycle de vie de développement du système ainsi que le processus de gestion de la configuration de ces éléments; d) définit les processus de gestion des correctifs pour les logiciels personnalisés utilisés dans la SAE, dont : I. la détermination, le signalement et la correction des failles dans les logiciels personnalisés, II. la mise à l'essai des mises à jour de logiciels visant à corriger les failles afin d'en vérifier l'efficacité et les effets secondaires possibles sur la SAE avant l'installation, e) iii) l'intégration de correctifs des failles dans le processus de gestion de la configuration de la SAE; f) définit les processus de gestion des correctifs pour les composantes de la SAE, dont : I. s'assurer que la version la plus récente des applications et des systèmes d'exploitation est utilisée, II. veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement, III. établir l'ordre de priorité des correctifs critiques à l'aide d'une approche fondée sur le risque, IV. mettre hors ligne et remettre en ligne des applications,

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		V. harmoniser les niveaux de criticité avec les correctifs, selon les directives du gouvernement du Canada; VI. attribuer une cote aux vulnérabilités qui s'appuie sur la deuxième version du Common Vulnerability Scoring System (CVSS), VII. appliquer une méthodologie de mise à l'essai et de vérification pour s'assurer que les correctifs ont été mis en œuvre correctement, VIII. aviser le gouvernement du Canada des vulnérabilités liées à la configuration qui permettraient à une personne non autorisée de compromettre la confidentialité, l'intégrité ou la disponibilité de la SAE.
E2.39	Gestion de la configuration	L'entrepreneur doit fournir au gouvernement du Canada un processus de gestion du changement pour la SAE, qui indique : a) les pouvoirs de l'entrepreneur en matière de gestion du changement; b) les rôles et les responsabilités des ressources de l'entrepreneur en matière de gestion du changement; c) la façon dont l'entrepreneur utilisera le processus de gestion du changement pour faciliter l'élaboration de la SAE (p. ex. concept des opérations); d) la méthode employée pour distinguer les éléments de configuration; e) la méthode de détermination des éléments de configuration; f) les moyens de détermination des éléments de configuration tout au long du cycle de vie de développement du système ainsi que le processus de gestion de la configuration de ces éléments.
E2.40	Planification d'urgence	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité relatives à la SAE qui définissent les rôles et les responsabilités opérationnels en matière de planification d'urgence.
E2.41	Planification d'urgence	L'entrepreneur doit, en collaboration avec le gouvernement du Canada, établir les priorités nationales en matière de restauration pour ce qui est de la SAE selon leur ordre de préséance, conformément aux directives du gouvernement du Canada.
E2.42	Planification d'urgence	L'entrepreneur doit : a) tester les données de sauvegarde de la SAE chaque mois afin de vérifier la fiabilité des supports et l'intégrité des données; b) utiliser un échantillon de données de sauvegarde de la SAE lors de la restauration des fonctions de ce dernier, dans le cadre de la mise à l'essai du plan de continuité des services.
E2.43	Planification d'urgence	L'entrepreneur doit conserver des copies de sauvegarde des logiciels du système d'exploitation, des logiciels de base critiques et du répertoire des composantes dans une installation distincte ou un contenant classé résistant au feu qui n'est pas situé dans les mêmes locaux que la SAE.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.44	Planification d'urgence	L'entrepreneur doit restaurer la SAE selon un état précédent connu après une interruption, une compromission ou une panne.
E2.45	Identification et authentification	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité qui définissent les rôles et les responsabilités opérationnels pour satisfaire aux exigences en matière d'identification et d'authentification précisées dans le présent énoncé des travaux.
E2.46	Identification et authentification	La SAE doit : a) identifier et authentifier les opérateurs de manière unique (ou les processus agissant au nom des opérateurs); b) attribuer un nom d'utilisateur et un mot de passe aux comptes en respectant les exigences de l'assurance de niveau 2 décrites dans le document ITSG-31 (https://www.cse-cst.gc.ca/fr/node/267/html/22784); c) permettre la sélection d'une question et d'une réponse pour la récupération du mot de passe; d) prévoir des mots de passe temporaires uniques pour l'inscription et la récupération de mots de passe; e) veiller à ce que les mots de passe temporaires uniques aient une période de validité pouvant être configurée, selon les directives du gouvernement du Canada; f) voir à ce que les mots de passe temporaires uniques soient aléatoires pour qu'ils ne soient pas prévisibles, comme l'a approuvé le gouvernement du Canada; g) permettre l'envoi d'avis automatiques indiquant l'expiration prochaine du mot de passe, selon les directives du gouvernement du Canada; h) prévoir des politiques et des processus de récupération de mots de passe; i) authentifier tout accès du client aux logiciels de la SAE.
E2.47	Identification et authentification	Les services de GIJIA de la SAE doivent permettre d'associer et de dissocier un ou plusieurs justificatifs d'identité à un compte individuel. (Par exemple, une personne pourrait utiliser son justificatif d'identité de niveau 2 de la SAE pour accéder à la Solution à titre d'utilisateur, et utiliser un autre justificatif d'identité X.509 pour accéder à la Solution afin d'exécuter des fonctions administratives.).
E2.48	Identification et authentification	La SAE doit : a) effectuer une authentification à deux facteurs à l'aide d'un jeton cryptographique matériel pour tous les comptes des opérateurs, conformément au document ITSG-31 du CSTC (https://www.cse-cst.gc.ca/fr/node/267/html/22784); b) effectuer une authentification mutuelle des appareils mobiles d'opérateurs qui sont connectés au réseau et accepter uniquement les appareils mobiles d'opérateurs autorisés.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.49	Identification et authentification	L'entrepreneur doit gérer les comptes des opérateurs de la SAE : a) en déterminant les types de comptes (c.-à-d. individuel, collectif, relatif à un système, à un appareil ou à une application, invité/anonyme, et temporaire); b) en établissant les conditions pour l'adhésion à des groupes; c) en déterminant les opérateurs autorisés de la SAE et en précisant les droits d'accès; d) en demandant les approbations requises pour les demandes d'établissement de comptes; e) en sélectionnant un identifiant qui identifie uniquement l'opérateur ou l'appareil; f) en attribuant l'identifiant de l'opérateur à la partie visée ou l'identifiant d'appareil à l'appareil visé; g) en établissant, en activant, en modifiant, en désactivant et en supprimant les comptes; h) en autorisant et en surveillant précisément l'utilisation des comptes temporaires et des comptes d'invités/comptes anonymes; i) en avisant l'administrateur des comptes lorsqu'un compte temporaire n'est plus requis et lorsque les opérateurs de la SAE quittent leur emploi ou sont mutés, ou lorsque des changements sont apportés à l'utilisation de la SAE ou au principe du besoin de connaître ou au principe du besoin de partager; j) en veillant à ce que les identifiants ne soient pas réutilisés durant au moins un an; k) en désactivant : i) les comptes temporaires qui ne sont plus requis; ii) les comptes des opérateurs qui ont quitté leur emploi ou qui ont été mutés; iii) les comptes après un certain nombre de jours d'inactivité, selon les directives du gouvernement du Canada, iv) les comptes temporaires et les comptes d'urgence après une période donnée; l) en accordant un accès à la SAE selon : i) une autorisation d'accès valide, ii) l'utilisation prévue du système; iii) d'autres exigences de l'entrepreneur ou du gouvernement du Canada; m) en révisant les comptes au moins une fois par mois; n) en verrouillant les comptes après dix tentatives d'ouverture de session infructueuses dans un délai de cinq minutes; o) en gardant les comptes verrouillés jusqu'à ce qu'ils soient déverrouillés manuellement par un autre opérateur.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.50	Identification et authentification	Les services de GIJIA de la SAE doivent consigner les événements suivants : a) création d'un compte; b) modification d'un compte; c) désactivation d'un compte; d) clôture d'un compte; e) en ce qui concerne l'assurance d'authentification de niveau 3, décrite dans le document ITSG-31 (https://www.cse-cst.gc.ca/fr/node/267/html/22784) : (i) changement de mots de passe, (ii) enregistrement des justificatifs d'identité, (iii) récupération de mots de passe, (iv) expiration de justificatifs d'identité.
E2.51	Identification et authentification	SUPPRIMER
E2.52	Identification et authentification	L'entrepreneur doit gérer les authentifiants des opérateurs par les moyens suivants : a) en vérifiant, lors de la transmission initiale des authentifiants, l'identité de la personne recevant l'authentifiant; b) en établissant le contenu de l'authentifiant initial pour ce qui est des authentifiants définis par l'entrepreneur; c) en s'assurant que la résistance des mécanismes des authentifiants est suffisante pour l'utilisation prévue de ceux-ci; d) en établissant et en mettant en œuvre des procédures administratives pour la transmission des authentifiants initiaux, les authentifiants perdus, compromis ou endommagés, et la révocation des authentifiants; e) en modifiant le contenu par défaut des authentifiants dès l'installation des composantes de la SAE; f) en établissant des restrictions relatives à la durée de vie minimale et maximale, et des conditions de réutilisation des authentifiants; g) en modifiant ou en mettant à jour les authentifiants à un intervalle ne dépassant pas 180 jours; h) en protégeant le contenu des authentifiants contre toute divulgation et modification non autorisées; i) en exigeant que les opérateurs prennent des mesures précises pour protéger les authentifiants.
E2.53	Identification et authentification	La SAE doit, aux fins de l'authentification par mot de passe : a) exiger des mots de passe ayant une complexité minimale, c'est-à-dire sensibles à la casse et composés de 15 caractères, dont au moins une majuscule, une minuscule, un chiffre et un caractère spécial; b) chiffrer les mots de passe lors du stockage et de la transmission; c) exiger des mots de passe ayant une durée de vie maximale de 90 jours; d) interdire la réutilisation des dix derniers mots de passe.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.54	Identification et authentification	Les services de GIJIA de la SAE doivent : a) fournir à l'utilisateur une liste de vérification, qui précise les règles que doit respecter un mot de passe, et cocher ces règles à mesure qu'elles sont respectées lorsque l'utilisateur saisit son mot de passe; b) communiquer à l'utilisateur les règles relatives aux mots de passe établies par le gouvernement du Canada, dont : i) le nombre minimal de caractères, ii) le nombre minimal de majuscules et de minuscules, iii) le nombre minimal de caractères spéciaux, iv) le nombre minimal de caractères alphanumériques, v) les mots trouvés dans un dictionnaire (anglais et français), vi) l'historique de réutilisation des mots de passe, vii) la durée de vie maximale des mots de passe.
E2.55	Identification et authentification	L'entrepreneur doit exiger que le processus d'inscription permettant aux opérateurs de la SAE de recevoir des identifiants ou des authentifiants soit réalisé en personne devant l'autorité d'enregistrement désignée avec l'autorisation d'un représentant désigné par le représentant de l'entrepreneur (p. ex. un superviseur).
E2.56	Identification et authentification	La SAE ne doit pas permettre la transmission de mots de passe en clair à partir de l'un ou l'autre des réseaux.
E2.57	Identification et authentification	L'entrepreneur ne doit pas permettre l'intégration d'authentifiants statiques non chiffrés dans les applications de la SAE ou des scripts d'accès, ou le stockage d'authentifiants dans des touches de fonction.
E2.58	Identification et authentification	La SAE doit occulter la rétroaction des données d'authentification des opérateurs (p. ex. en masquant les champs de mot de passe) pendant le processus d'authentification.
E2.59	Identification et authentification	L'entrepreneur doit établir un processus d'autorisation du personnel de maintenance, notamment : a) tenir à jour une liste des organisations et du personnel responsables de la maintenance; b) s'assurer que le personnel de maintenance du service de la SAE possède les autorisations d'accès requises; c) veiller à ce que le personnel désigné possédant les autorisations d'accès requises supervise les activités de maintenance lorsque le personnel de maintenance ne possède pas les autorisations d'accès requises.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.60	Intervention en cas d'incident	L'entrepreneur doit : a) présenter au gouvernement du Canada les procédures opérationnelles de sécurité qui définissent les rôles et les responsabilités opérationnels pour satisfaire aux exigences en matière d'intervention en cas d'incident précisées dans le présent énoncé des travaux; b) mettre en œuvre et mettre à l'essai le plan de continuité des services (ensemble des processus, des procédures, des rôles, des responsabilités, etc.) tous les ans, et transmettre les résultats des essais au gouvernement du Canada dans un délai de dix (10) jours ouvrables du gouvernement fédéral suivant l'achèvement de la mise à l'essai du plan de continuité des services; c) soumettre au gouvernement du Canada un plan de continuité des services qui comprend : i. un plan détaillé et des processus consignés de restauration de la SAE, ii. des détails sur le plan de communication établi entre le gouvernement du Canada et ses fournisseurs, iii. des détails sur le plan et les processus de transfert des fonctions d'exploitation, de gestion et d'administration à un centre des opérations secondaire, iv. les stratégies de sauvegarde pour les installations des centres de données, les installations du réseau, les systèmes de soutien opérationnel et les données, et les principales composantes de service, v. les moyens que l'entrepreneur prendra pour s'assurer que ses fournisseurs ont des plans de continuité des services en place, vi. une description du processus utilisé pour mettre à l'essai le plan de continuité des services, vii. les mesures que l'entrepreneur prendra si un de ses principaux fournisseurs met fin à ses activités, viii. les mesures que l'entrepreneur prendra si un des fabricants d'équipement d'origine n'est plus considéré comme un fabricant de confiance ou un fabricant d'équipement d'origine par le gouvernement du Canada.
E2.61	Intervention en cas d'incident	L'entrepreneur doit présenter une version définitive du plan de continuité des services dans les quinze jours ouvrables du gouvernement fédéral suivant la réception des commentaires du gouvernement du Canada sur le plan de continuité des services provisoire.
E2.62	Intervention en cas d'incident	L'entrepreneur doit mettre en œuvre le plan de continuité des services (ensemble des processus, des procédures, des rôles, des responsabilités, etc.) Et toute mise à jour annuelle ultérieure dans un délai de 60 jours ouvrables du gouvernement fédéral suivant l'acceptation du plan par gouvernement du Canada.
E2.63	Intervention en cas d'incident	L'entrepreneur doit fournir au gouvernement du Canada, dans les 40 jours ouvrables du gouvernement fédéral suivant une demande, la preuve établie il y a moins d'un an (p. ex. résultats d'essai, évaluations et vérifications) que le plan de continuité des services a été convenablement mis en œuvre, qu'il fonctionne comme prévu, qu'il produit les résultats escomptés et qu'il satisfait aux exigences du gouvernement du Canada en matière de continuité des services.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.64	Intervention en cas d'incident	Si l'entrepreneur détermine qu'il lui faudra plus de 40 jours ouvrables du gouvernement fédéral pour présenter la preuve demandée pour le plan de continuité des services, il doit en aviser le Canada au plus tard cinq jours ouvrables du gouvernement fédéral après la demande de preuve initiale et solliciter par écrit une prolongation en fournissant la justification appropriée. La décision d'accorder ou non une prolongation sera laissée à la seule discrétion du Canada. Le certificat de conformité est une preuve reconnue par le Canada.
E2.65	Intervention en cas d'incident	L'entrepreneur doit répondre aux alertes, aux conseils et aux directives de sécurité pour le système d'information de la part d'organisations externes désignées et approuvées par le gouvernement du Canada de manière continue, notamment : a) surveiller constamment les alertes, les avis et les directives de sécurité; b) préparer les alertes, les avis et les directives de sécurité internes jugés nécessaires ou demandés par le gouvernement du Canada; c) diffuser les alertes, les avis et les directives de sécurité auprès des opérateurs ayant des responsabilités en matière de sécurité; d) mettre en œuvre les directives de sécurité conformément aux délais établis, ou aviser le gouvernement du Canada du niveau du problème de non-conformité;
E2.66	Intervention en cas d'incident	En plus des sources de renseignement sur les menaces et les incidents cybernétiques analysées dans le cadre de ses opérations de routine, l'entrepreneur doit surveiller les publications sur le même sujet provenant des sources désignées par le Canada, comme le Centre canadien de réponse aux incidents cybernétiques [CCRIC](http://www.securitepublique.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-fr.aspx).
E2.67	Intervention en cas d'incident	L'entrepreneur doit mettre sur pied un Centre des opérations de sécurité (COP) avant la fin de la phase de stabilité opérationnelle, et fournir les ressources nécessaires à la surveillance et à la résolution centralisées (24 heures sur 24, 7 jours sur 7, 365 jours par année) des incidents de sécurité liés à la SAE.
E2.68	Intervention en cas d'incident	Le Centre des opérations de sécurité doit faire ce qui suit : a) coordonner l'intervention en cas d'incident de sécurité en étroite collaboration avec le gouvernement du Canada; b) fournir une ligne téléphonique unique et réservée qui est accessible en tout temps et exploitée dans la langue officielle du Canada (français ou anglais) tel que demandée par l'appelant; c) agir comme point de contact pour les communications avec les représentants du gouvernement du Canada au sujet des incidents de sécurité; d) ne pas perturber l'exploitation de la SAE en cas de panne du Centre des opérations de sécurité (COP) de l'entrepreneur; e) aviser le gouvernement du Canada dans un délai de 15 minutes en cas de panne et fournir le nom de la personne-ressource avec qui le gouvernement du Canada peut communiquer pendant la panne.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.69	Intervention en cas d'incident	Le COP doit travailler avec le Centre des opérations de protection (COP) du gouvernement du Canada dans le cadre des activités suivantes : a) intégration des processus; b) surveillance; c) gestion des incidents de sécurité et intervention en cas d'incident de sécurité; d) audit des incidents; e) Le confinement, l'éradication et la récupération en cas d'incident de sécurité, qui comprennent : i. la capacité à dépêcher l'équipe de reprise après incident de sécurité de la TI sur le site de l'entrepreneur, ii. Permettre au gouvernement du Canada d'assurer l'orientation et la coordination sur place
E2.70	Intervention en cas d'incident	L'entrepreneur doit automatiquement transmettre par courriel sécurisé les renseignements sur les dossiers d'incident aux destinataires d'une liste de diffusion prédéfinie pour chaque incident lié à la SAE, selon les spécifications suivantes fournies par le gouvernement du Canada : a) les renseignements du dossier d'incident qui doivent apparaître dans le courriel sécurisé; b) la fréquence des mises à jour de la SAE; c) les listes de distribution; d) les critères de sélection des incidents (gravité, priorité, contenu du dossier d'incident).
E2.71	Intervention en cas d'incident	L'entrepreneur doit poursuivre l'envoi automatique de courriels sécurisés lorsqu'un dossier d'incident est mis à jour, et ce, jusqu'à ce que le dossier d'incident soit clos ou que le gouvernement du Canada annule la déclaration automatique des mises à jour.
E2.72	Intervention en cas d'incident	L'entrepreneur doit mettre en place des mesures d'atténuation (p. ex. des mesures de blocage à l'aide du pare-feu, de signatures des services de détection et de prévention d'intrusion, de suppression des logiciels malveillants) afin de maîtriser un incident de sécurité, d'assurer une protection contre les menaces cybernétiques et d'éliminer les vulnérabilités.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.73	Intervention en cas d'incident	L'entrepreneur doit présenter un rapport rétrospectif sur tout incident de sécurité au gouvernement du Canada dans les 72 heures suivant la demande de ce dernier, en incluant notamment : a) le numéro de l'incident de sécurité; b) la date d'ouverture du dossier d'incident de sécurité; c) la date de fermeture du dossier d'incident de sécurité; d) la description de l'incident de sécurité; e) la portée de l'incident de sécurité; f) la chaîne d'événements/le déroulement; g) les mesures prises par l'entrepreneur; h) les leçons apprises; i) les limites et les problèmes relatifs à la SAE; j) des recommandations en vue d'améliorer la SAE.
E2.74	Intervention en cas d'incident	L'entrepreneur doit assurer une surveillance continue des événements survenant sur la SAE afin de : a) détecter les attaques, les incidents et les événements anormaux touchant la SAE; b) relever toute utilisation et tout accès non autorisés aux données et aux composantes de la SAE; c) répondre aux menaces et aux attaques contre la SAE, les contenir et veiller à la reprise du service.
E2.75	Intervention en cas d'incident	L'entrepreneur doit donner de la formation aux opérateurs de la SAE au sujet de leurs rôles et responsabilités en matière d'intervention en cas d'incident, et donner une formation d'appoint tous les ans.
E2.76	Intervention en cas d'incident	L'entrepreneur doit mettre à l'essai le processus d'intervention en cas d'incident de la SAE, au moins tous les ans, à l'aide de scripts de test complets, afin de déterminer l'efficacité de l'intervention en cas d'incident, y compris : a) consigner les résultats des essais; b) examiner les résultats des essais avec le gouvernement du Canada; c) mettre en œuvre des mesures correctives selon les directives du Canada dans le délai convenu avec lui.
E2.77	Intervention en cas d'incident	L'entrepreneur doit s'assurer que la posture de sécurité de la SAE est maintenue en assurant de façon constante : a) la surveillance des menaces et des vulnérabilités; b) une surveillance continue des activités malveillantes et des accès non autorisés; c) l'adoption, s'il y a lieu, de contre-mesures proactives, y compris des mesures préventives et des mesures d'intervention pour atténuer les menaces.
E2.78	Intervention en cas d'incident	Le Centre des opérations de sécurité doit :

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		a) accepter les courriels que les représentants autorisés du gouvernement du Canada envoient à la boîte de réception fournie par l'entrepreneur. Celle-ci doit être dotée d'une fonction de réponse automatique pour accuser réception du courriel; b) accuser réception des courriels provenant d'adresses électroniques de la SAE autorisées par le Canada dans les 15 minutes suivant leur réception, et ce, en tout temps; c) authentifier l'identité du demandeur au moyen d'un processus approuvé par le Canada.
E2.79	Intervention en cas d'incident	L'entrepreneur doit créer un ou plusieurs dossiers d'incident pour chaque incident qu'il relève ou qui est signalé par le gouvernement du Canada.
E2.80	Intervention en cas d'incident	L'entrepreneur doit séparer physiquement ou logiquement l'information sur les incidents de sécurité de l'information sur tous les autres types d'incident. Tout renseignement sur les enquêtes liées à la sécurité généré dans le cadre du dossier doit être enregistré dans l'entreposage dédié du gouvernement du Canada.
E2.81	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le gouvernement du Canada en signale un, l'entrepreneur doit ouvrir un dossier d'incident dans un délai maximal de cinq minutes
E2.82	Intervention en cas d'incident	L'entrepreneur doit passer en revue les leçons apprises des activités de traitement des incidents en cours et intégrer les mesures correctives subséquentes dans les procédures d'intervention en cas d'incident, la formation, la mise à l'essai et les exercices.
E2.83	Intervention en cas d'incident	Les dossiers d'incident de sécurité doivent inclure les renseignements supplémentaires suivants : a) le type et la description de l'attaque ou de l'événement; b) une indication du succès ou de l'échec de l'attaque, et ses répercussions; c) la portée de l'attaque (d'une organisation ou de nombreuses organisations); d) le nombre estimatif de systèmes touchés par organisation; e) une liste des systèmes touchés par organisation; f) la source ou l'origine apparente de l'attaque/de l'incident/de l'événement; g) la date et l'heure de l'attaque/de l'incident/de l'événement; h) le secteur/degré de préjudice estimatif; i) l'estimation des impacts; j) la durée de l'attaque/de l'incident/de l'événement; k) les mesures prises; l) l'état des mesures d'atténuation; m) les registres applicables ou les données probantes.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.84	Intervention en cas d'incident	L'entrepreneur doit déclarer en tant qu'incident toutes les violations suspectes à la protection des renseignements personnels et à la sécurité relatives au service à la SAE.
E2.85	Intervention en cas d'incident	L'entrepreneur doit fournir tous les éléments de preuve associés à un incident de sécurité dans le format de fichier commercial et le délai précisés par le gouvernement du Canada, dont : a) les résultats de la recherche dans les registres historiques et les dossiers de vérification associés à un ou plusieurs partenaires selon les critères fournis par le gouvernement du Canada; b) les résultats de l'analyse des registres et des dossiers de vérification associés à un ou à plusieurs organismes selon les critères établis par le gouvernement du Canada; c) les registres et les dossiers de vérification selon les critères fournis par le gouvernement du Canada; d) des renseignements ou des données supplémentaires, selon les directives du gouvernement du Canada;
E2.86	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le gouvernement du Canada en signale un, l'entrepreneur doit ouvrir un dossier d'incident dans un délai maximal de cinq minutes
E2.87	Intervention en cas d'incident	L'entrepreneur doit mettre à jour l'incident dans les cinq minutes suivant la modification de l'état d'un incident de grande priorité et dans les quinze minutes suivant la modification de l'état de tout autre type d'incident.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.88	Intervention en cas d'incident	Les dossiers d'incident de l'entrepreneur doivent comprendre notamment les champs d'information suivants, lesquels doivent être actualisés : a) le numéro de dossier attribué par l'entrepreneur; b) la description de l'incident; c) les coordonnées de la personne ayant fait état de l'incident (nom, numéro de téléphone et adresse électronique); d) la langue de la personne qui a soumis l'incident; e) les dossiers d'incident connexes; f) la date et l'heure d'ouverture du dossier d'incident; g) la date et l'heure de fermeture du dossier d'incident; h) le type du dossier d'incident (p. ex. production, essai de fonctionnalité, essai de rendement, sécurité), selon les directives du gouvernement du Canada; i) la gravité du dossier d'incident; j) les répercussions du dossier d'incident; k) l'ordre de priorité du dossier d'incident; l) l'état du dossier d'incident (c.-à-d. ouvert, fermé, en cours, suspendu, annulé, etc.); m) le processus d'escalade du dossier d'incident; n) le numéro du dossier d'incident interne du gouvernement du Canada; o) les fonctions de service touchées; p) les points de prestation de service touchés; q) les coordonnées de l'entrepreneur (nom, numéro de téléphone et adresse électronique); r) l'identifiant des partenaires (s'il y a lieu); s) les interactions avec les tierces parties; t) le journal des activités; u) la cause fondamentale de l'incident (si possible); v) le temps estimatif requis pour résoudre l'incident (mis à jour toutes les 15 minutes); w) la description de la résolution; x) la durée de la panne (dans le cas des dossiers fermés seulement)
E2.89	Intervention en cas d'incident	Lorsque l'entrepreneur détecte un incident ou que le gouvernement du Canada en signale un, l'entrepreneur doit ouvrir un dossier d'incident dans un délai maximal de cinq minutes
E2.90	Intervention en cas d'incident	L'entrepreneur doit mettre à jour l'incident dans les cinq minutes suivant la modification de l'état d'un incident de grande priorité et dans les quinze minutes suivant la modification de l'état de tout autre type d'incident.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.91	Intervention en cas d'incident	L'entrepreneur doit aviser le gouvernement du Canada, par téléphone et par courriel (7 jours sur 7, 24 heures sur 24, 365 jours par année), selon l'ordre de priorité établi par le gouvernement du Canada, de tout incident de sécurité réel ou soupçonné, notamment : a) les attaques de logiciels rançonneurs; b) les attaques par déni de services; c) les maliciels; d) l'ingénierie sociale; e) l'intrusion ou l'accès non autorisés; f) les fuites de renseignements; g) toutes les autres violations de la sécurité ou cybermenaces ciblant le gouvernement du Canada.
E2.92	Intervention en cas d'incident	L'entrepreneur doit divulguer au Canada tous les renseignements et données qu'il possède relativement à la SAE ou qui se rapportent à un incident de sécurité.
E2.93	Intervention en cas d'incident	L'entrepreneur doit fournir un portail sécurisé de gestion de la sécurité afin de permettre au gouvernement du Canada de visualiser tout renseignement relatif à la sécurité à partir de la SAE. Ces renseignements comprennent notamment : a) les rapports d'incident de sécurité, les rapports post mortem, les rapports ad hoc et les données probantes connexes; b) les dossiers d'incident de sécurité; c) les rapports sur les activités des utilisateurs; d) les rapports sur les activités des opérateurs; e) les rapports sur l'accès au système; f) les rapports sur l'audit de la configuration; g) les rapports sur les changements à la configuration; h) les rapports sur la surveillance de l'intégrité des fichiers; i) les rapports sur le répertoire; j) les rapports sur les vulnérabilités; k) les rapports sur les changements à la configuration; l) les demandes de changement d'urgence et les demandes de changement; m) les correctifs généraux et les correctifs de sécurité mis en œuvre; n) des renseignements confirmant ou non le blocage ou le filtrage des achats électroniques, et la durée du blocage ou du filtrage; o) d'autres documents justificatifs (p. ex. liste blanche, liste noire).

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.94	Intervention en cas d'incident	L'entrepreneur doit déclarer en tant qu'incident toutes les violations suspectes à la protection des renseignements personnels et à la sécurité relatives au service à la SAE.
E2.95	Intervention en cas d'incident	Les réunions sur les incidents de sécurité ou les questions de sécurité déterminées par le gouvernement du Canada doivent être tenues en personne dans la région de la capitale nationale (RCN) durant les heures normales d'ouverture (de 8 h à 17 h, heure normale de l'Est), du lundi au vendredi et durant les heures de travail en dehors de cette période, selon ce dont conviennent l'entrepreneur et le gouvernement du Canada.
E2.96	Intervention en cas d'incident	L'entrepreneur doit être disponible pour participer à une séance d'information sur les incidents de sécurité donnée par le gouvernement du Canada (p. ex. séance d'information confidentielle).
E2.97	Intervention en cas d'incident	L'entrepreneur doit avoir des procédures judiciaires et des mesures de protection en vigueur concernant ce qui suit : a) la tenue d'une chaîne de possession pour tous les renseignements sur la vérification; b) la collecte, la conservation et la présentation des éléments de preuve démontrant l'intégrité de la preuve.
E2.98	Intervention en cas d'incident	L'entrepreneur doit élaborer un plan d'intervention en cas d'incident qui inclut : a) la façon dont l'entrepreneur prévoit déterminer les incidents de sécurité, établir des rapports sur ceux-ci et les acheminer au palier hiérarchique supérieur; b) une feuille de route pour la mise en œuvre de la capacité d'intervention en cas d'incident de sécurité, notamment pour ce qui est de la préparation, de la détection, de l'analyse, du confinement et du rétablissement; c) une description de la structure et de l'organisation de la capacité d'intervention en cas d'incident de sécurité; d) une approche de haut niveau concernant l'intégration de la capacité d'intervention en cas d'incident de sécurité dans l'ensemble de l'organisation de l'entrepreneur; e) une définition des incidents de sécurité à signaler; f) une définition des mesures utilisées pour évaluer la capacité d'intervention en cas d'incident de sécurité; g) une définition des ressources et du soutien de la direction nécessaires pour maintenir et améliorer la capacité d'intervention en cas d'incident de sécurité.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.99	Maintenance du système	L'entrepreneur doit procéder à la maintenance dirigée : a) planifier, exécuter et consigner la maintenance et les réparations des composantes de la SAE conformément aux spécifications du fabricant ou du vendeur, et en examinant les dossiers de maintenance; b) en dirigeant toutes les activités de maintenance, qu'elles soient exécutées sur place ou à distance, et que l'équipement soit entretenu sur place ou dans un autre emplacement; c) demander l'autorisation explicite d'un représentant désigné de l'entrepreneur avant de retirer certaines composantes de la SAE du centre de données de l'entrepreneur aux fins de maintenance ou de réparations hors site; d) en nettoyant l'équipement afin d'effacer toutes les données des supports connexes avant de le retirer des installations de l'entrepreneur aux fins de maintenance ou de réparations hors site; e) vérifier tous les contrôles de sécurité susceptibles d'être perturbés pour s'assurer qu'ils fonctionnent toujours correctement à la suite des activités de maintenance ou de réparation.
E2.100	Maintenance du système	L'entrepreneur doit approuver, contrôler, surveiller et entretenir de façon continue le matériel et les logiciels utilisés pour la maintenance de la SAE, en particulier pour ce qui est du diagnostic et des réparations (p. ex. outils matériels ou logiciels introduits pour effectuer une activité de maintenance en particulier).
E2.101	Maintenance du système	L'entrepreneur doit : a) vérifier que tous les supports d'information contenant des programmes de diagnostic et d'essai ne comportent aucun programme malveillant avant d'autoriser leur utilisation dans les composantes de la SAE. b) s'assurer que l'équipement ne contient aucun renseignement sur la SAE; c) nettoyer ou détruire l'équipement de la SAE; d) conserver l'équipement de la SAE à son installation ou obtenir une exemption d'une autorité contractante désignée de la SAE autorisant précisément l'enlèvement de l'équipement de l'installation de la SAE.
E2.102	Maintenance du système	L'entrepreneur doit autoriser, surveiller et contrôler les activités de maintenance et de diagnostic de la SAE : a) en permettant l'utilisation des outils de maintenance et de diagnostic approuvés par le gouvernement du Canada (à discuter); b) en employant de solides techniques d'identification et d'authentification étroitement liées à l'utilisateur dans l'établissement de séances de maintenance et de diagnostic, et en isolant ces séances des autres séances du réseau dans l'infrastructure de la SAE par l'un des moyens suivants : (i) en utilisant des voies de communication séparées physiquement ou logiquement, (ii) en utilisant des voies de communication dont la séparation logique est fondée sur des modules et des algorithmes cryptographiques approuvés par le CSTC (se reporter à la sous-section Normes de chiffrement); c) en consignant les séances de maintenance et de diagnostic; d) en demandant au personnel désigné d'examiner les dossiers de maintenance et de diagnostic.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.103	Maintenance du système	L'entrepreneur doit établir un processus d'autorisation du personnel de maintenance, notamment : a) tenir à jour une liste des organisations et du personnel responsables de la maintenance; b) s'assurer que le personnel responsable de la maintenance de la SAE possède les autorisations d'accès requises; c) veiller à ce que le personnel désigné possédant les autorisations d'accès requises supervise les activités de maintenance lorsque le personnel de maintenance ne possède pas les autorisations d'accès requises.
E2.104	Protection des supports	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité qui définissent les exigences en matière de protection des supports, précisées dans le présent énoncé des travaux.
E2.105	Protection des supports	L'entrepreneur doit : a) limiter aux opérateurs autorisés l'accès aux supports de TI (numériques et non numériques) qui contiennent des données sur la SAE; b) utiliser des mécanismes pour vérifier les tentatives d'accès et les accès accordés
E2.106	Protection des supports	Conformément aux dispositions du contrat, l'entrepreneur doit marquer les supports de TI amovibles qui contiennent des renseignements du gouvernement du Canada indiquant les restrictions de diffusion, les oppositions et les marquages de sécurité applicables (le cas échéant) des renseignements.
E2.107	Protection des supports	L'entrepreneur doit contrôler physiquement et logiquement les supports de TI contenant des données sur la SAE et les stocker de façon sécuritaire, conformément : a) aux pratiques exemplaires de l'industrie; b) à l'équipement, aux techniques et aux procédures approuvés par le gouvernement du Canada pour la destruction des données (sur place ou hors site) comprenant sans s'y limiter : Entreposage • ordinateurs sécurisés DASCO, serveur de fichiers, armoires pour télécopieur; • étagères mobiles sécurisées, onglet (à rayonnage mobile G1-028); • armoires de rangement de renseignements DASCO; • classeurs de sécurité (deux et quatre tiroirs), Comité consultatif sur la sécurité matérielle (CCSM) 101; • coffres-forts pour opérations mobiles de types A et B; Fournisseurs de services de destruction • Services de destruction mobile Iron Mountain (MDS-35-GTI);

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		• Installation de destruction RECALL (installation de Toronto); • Installations de destruction Iron Mountain (Calgary); • Installations de destruction Iron Mountain (Calgary); • Installation de destruction Absolute Data Destruction (Toronto) Déchiqueteuses • Dahle 20831 EC • Kobra 400 HS ES (400 HS AO ES) • HSM 411.2 HS • Roto 600HS • Fellowes HS-1010
E2.108	Protection des supports	L'entrepreneur doit utiliser des mécanismes cryptographiques pour protéger les renseignements entreposés qui sont approuvés par le gouvernement du Canada et qui sont conformes aux directives du CSTC (ITSG-111 https://www.cse-cst.gc.ca/fr/node/1428/html/25015).
E2.109	Protection des supports	L'entrepreneur doit nettoyer et vérifier les supports de TI contenant des données de la SAE (numériques et non numériques), avant leur élimination, leur retrait du contrôle de l'organisation ou leur retrait en vue de leur réutilisation.
E2.110	Protection des supports	L'entrepreneur doit assurer le suivi et le contrôle des activités d'épuration des supports et vérifier celles-ci en : a) mener les activités d'épuration des supports conformément aux exigences énoncées dans le document ITSG-06 (https://www.cse-cst.gc.ca/fr/node/270/html/10572) pour les renseignements de niveau protégé B. b) consignant les activités d'épuration des supports; c) mettant à l'essai l'équipement et la procédure d'épuration afin de vérifier le rendement au moins une fois par année; d) nettoyer les appareils de stockage usagés qui ont été réaffectés avant de les raccorder au service de la Solution d'achats électroniques.
E2.111	Protection physique et environnementale	L'entrepreneur doit présenter au gouvernement du Canada les procédures opérationnelles de sécurité qui définissent les exigences en matière de protection physique et environnementale précisées dans le présent énoncé des travaux.
E2.112	Protection physique et environnementale	L'entrepreneur doit autoriser, surveiller et contrôler toutes les composantes qui entrent dans les installations de la SAE et qui en sortent, et il doit tenir des dossiers sur ces composantes et ces activités. Les dossiers doivent être fournis chaque mois et à la demande du gouvernement du Canada.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.113	Protection physique et environnementale	L'entrepreneur doit mettre en œuvre d'autres contrôles de gestion et de sécurité techniques, et contrôles opérationnels permettant d'atteindre les mêmes objectifs que les contrôles mis en place dans les installations de la SAE. La Direction de la sécurité industrielle canadienne ou la Direction de la sécurité industrielle internationale doit approuver le(s) site(s) de remplacement en même temps que les sites principaux.
E2.114	Sécurité du personnel	L'entrepreneur doit, lors de la cessation d'emploi d'un employé dont les tâches étaient liées à la SAE : a) mettre fin à l'accès physique de l'employé aux installations de la SAE; b) mettre fin à l'accès à la SAE, y compris l'accès à distance; c) récupérer tous les biens liés à la sécurité (p. ex. carte d'identité de l'employé, jeton d'authentification physique); d) effectuer une entrevue de fin d'emploi lors de la cessation d'emploi d'un employé; e) conserver l'accès à l'information et aux systèmes d'information organisationnels, conformément à la Norme sur la sécurité du personnel du Secrétariat du Conseil du Trésor (SCT), lors de la cessation d'emploi d'un employé.
E2.115	Sécurité du personnel	L'entrepreneur doit conclure des ententes afin d'accéder à la SAE ou aux données de la SAE dans les cas suivants : a) avant de se voir accorder un accès à la SAE ou aux données de la SAE, les opérateurs signent une entente d'accès qui présente le processus de sanction officiel en cas de non-respect des modalités de ladite entente; b) l'entrepreneur examine et met à jour les ententes d'accès visant la SAE ou les données de la SAE tous les deux ans.
E2.116	Sécurité du personnel	L'entrepreneur doit : a) avant de se voir accorder un accès à la SAE ou aux données de la SAE, s'assurer que les opérateurs signent une entente d'accès qui présente le processus de sanction officiel en cas de non-respect des modalités de ladite entente; b) donner aux opérateurs de la SAE une formation sur leurs responsabilités en matière de protection des renseignements personnels et de la confidentialité des données de la SAE conformément aux modalités du contrat de la SAE et aux sanctions prévues en cas de non-respect. L'entrepreneur doit donner une formation d'appoint deux fois par année.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.117	Évaluation des risques	L'entrepreneur doit fournir une évaluation de la vulnérabilité certifiée d'une tierce partie accompagnée des données brutes justifiant cette évaluation dans les 10 jours ouvrables du gouvernement fédéral suivant la demande du Canada. Cette évaluation portera sur : a) l'accès physique aux installations de la SAE (c.-à-d. installations de l'entrepreneur où est située la SAE de SPAC [matériel et logiciel]); b) l'accès au réseau de la SAE afin de permettre le balayage authentifié et non authentifié des composantes du réseau et des appareils de sécurité, à l'aide de l'équipement reconnu et approuvé du gouvernement du Canada ou de l'industrie; c) le soutien, durant la partie de l'évaluation de la vulnérabilité effectuée sur place, d'au moins une ressource technique qui connaît les aspects techniques de la SAE (c.-à-d. matériel, logiciel, composantes du réseau, appareil de sécurité, et leur configuration); d) la limitation de l'évaluation de la vulnérabilité du gouvernement du Canada aux activités de découverte et d'analyse dans la SAE, sans entreprendre d'activités perturbatrices ou destructives.
E2.118	Acquisition de systèmes et de services	À partir de la date à laquelle les vulnérabilités sont ciblées officiellement, l'entrepreneur doit, au minimum : a) atténuer toutes les vulnérabilités à risque élevé dans un délai de 10 jours; b) atténuer toutes les vulnérabilités à risque modéré dans un délai de 30 jours. c) corriger toutes les vulnérabilités dans un délai de 30 jours. Le Canada et l'entrepreneur doivent déterminer la cote de risque des vulnérabilités et convenir mutuellement de celle-ci.
E2.119	Acquisition de systèmes et de services	L'entrepreneur doit maintenir l'état d'autorisation de sécurité de la SAE par la surveillance soutenue et la vérification annuelle des exigences ayant été mises en œuvre en matière de sécurité en ce qui a trait aux services de la SAE, le tout afin de déterminer si les exigences en matière de sécurité du système d'information sont toujours efficaces au fil du temps, à la lumière des modifications qui sont apportées au service de la Solution d'achats électroniques et à son environnement opérationnel.
E2.120	Acquisition de systèmes et de services	L'entrepreneur doit fournir des preuves à l'appui des activités de maintien des autorisations dans les 30 jours suivant une demande du Canada, à la suite de tous les changements apportés à la SAE par l'entrepreneur.
E2.121	Acquisition de systèmes et de services	L'entrepreneur doit, à la demande du Canada et dans les 30 jours de celle-ci, mettre à jour les procédures opérationnelles de sécurité et démontrer leur mise en œuvre dans le cadre des activités de maintien des autorisations.
E2.122	Protection du système et des communications	L'entrepreneur doit inclure, dans les procédures opérationnelles de sécurité, une politique et des procédures visant à faciliter la mise en œuvre et la tenue à jour, des exigences en matière de protection du système et des communications,

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		qui sont précisées dans le présent énoncé des travaux et dans les normes applicables du gouvernement du Canada mentionnées dans cet énoncé des travaux.
E2.123	Protection du système et des communications	La SAE doit disposer de contrôles qui correspondent aux pratiques exemplaires de l'industrie pour gérer les attaques de type déni de service, conformément à ce qui a été convenu entre le gouvernement du Canada et l'entrepreneur par l'intermédiaire du processus d'évaluation et d'autorisation de sécurité.
E2.124	Protection du système et des communications	1) La conception des services de la SAE doit respecter les zones de sécurité de réseau, conformément aux documents ITSG-22 (https://www.cse-cst.gc.ca/fr/node/268/html/15236) et ITSG-38 (https://www.cse-cst.gc.ca/fr/node/266/html/25034). En outre, la SAE doit surveiller et contrôler les communications aux limites externes du système et aux principales limites internes de celui-ci en conformité avec les documents ITSG-22 (https://www.cse-cst.gc.ca/fr/node/268/html/15236) et ITSG-38 (https://www.cse-cst.gc.ca/fr/node/266/html/25034). 2) L'entrepreneur responsable de la SAE doit surveiller et analyser le trafic sur le réseau, en temps réel, pour détecter les attaques et les preuves relatives aux composantes compromises de la SAE. 3) L'entrepreneur responsable de la SAE doit détecter les attaques, notamment : a) les attaques de rançongiciels; b) les attaques par déni de service; c) les logiciels malveillants; d) l'ingénierie sociale; e) l'intrusion ou l'accès non autorisé; f) la violation de la sécurité de l'information; g) toutes les autres violations de la sécurité ou de cybermenaces ciblant le gouvernement du Canada.
E2.125	Protection du système et des communications	La SAE doit uniquement se brancher aux réseaux externes ou aux systèmes d'information précisés par le Canada au moyen d'interfaces à l'aide de dispositifs de protection des frontières, conformément aux documents ITSG-22 (https://www.cse-cst.gc.ca/fr/node/268/html/15236) et ITSG-38 (https://www.cse-cst.gc.ca/fr/node/266/html/25034).
E2.126	Protection du système et des communications	L'entrepreneur doit gérer activement toutes les connexions réseau aux services externes associées à la SAE, c'est-à-dire : a) refus par défaut de tout trafic sur le réseau; b) définition du trafic permis dans chaque connexion réseau (refus systématique et autorisation par exception); c) coupure de la connexion réseau associée à une séance de communication à la fin de la séance ou après un nombre défini de minutes d'inactivité selon les directives du gouvernement du Canada; d) consignation de chaque exception à la politique sur le flux du trafic en indiquant la nature et la durée du besoin; e) révision des exceptions à la politique sur le flux du trafic au moins une fois par année;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		f) suppression des exceptions à la politique sur le flux du trafic qui ne sont plus justifiées par un besoin opérationnel explicite; g) surveillance du trafic afin de détecter les activités ou les conditions non autorisées; h) au besoin, surveillance du trafic à certains points à l'intérieur du système (p. ex. les sous-réseaux, les sous-systèmes) pour découvrir des anomalies.
E2.127	Protection du système et des communications	L'entrepreneur doit empêcher que les appareils qu'il gère (p. ex. ordinateur portatif ou autre appareil utilisé à des fins administratives) qui sont connectés à la SAE établissent des communications à l'extérieur de cette voie de communication (p. ex. accéder à Internet à partir d'une connexion distincte disponible).
E2.128	Protection du système et des communications	La SAE doit détecter les fuites aussitôt que possible et aviser le Canada dès la détection.
E2.129	Protection du système et des communications	L'entrepreneur doit surveiller et analyser les composantes des hôtes (prévention et détection des intrusions en mode hôte) afin de détecter le plus rapidement possible les attaques et les preuves relatives aux hôtes compromis et en aviser le Canada.
E2.130	Protection du système et des communications	SUPPRIMER
E2.131	Protection du système et des communications	L'entrepreneur doit configurer les mesures de protection des limites (c.-à-d. pare-feu) au mode « interruption avec protection simultanée » (c.-à-d. interruption du trafic) dès qu'une défaillance survient.
E2.132	Protection du système et des communications	L'architecture opérationnelle de la SAE doit : a) permettre l'authentification mutuelle des connexions entre la SAE et les autres domaines, selon les directives du Canada et autoriser exclusivement l'échange d'information avec ces autres domaines en utilisant l'authentification mutuelle; b) garantir que l'intégrité et la confidentialité des données de la SAE, durant la transmission et en période d'arrêt, sont protégées à l'aide de solutions cryptographiques, sauf si elles sont protégées par d'autres mécanismes approuvés par le Canada.
E2.133	Protection du système et des communications	La SAE doit protéger l'intégrité et la confidentialité des données de la SAE durant la transmission et en période d'arrêt à l'aide des modules et des algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications du Canada (se reporter à la sous-section Normes de chiffrement), sauf si elles sont protégées par d'autres mesures de protection physique approuvées par le Canada.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.134	Protection du système et des communications	SUPPRIMER
E2.135	Protection du système et des communications	L'architecture opérationnelle de la SAE doit veiller à ce que : a) les solutions cryptographiques (p. ex. solutions de réseau privé virtuel, protocole TLS, modules logiciels, infrastructure à clés publiques et jetons d'authentification, s'il y a lieu) utilisées pour la SAE : i) utilisent des algorithmes cryptographiques, des tailles de clés cryptographiques ainsi que des cryptopériodes qui ont été approuvés par le CSTC et validés par le Programme de validation des algorithmes cryptographiques (http://csrc.nist.gov/groups/STM/cavp/), et qui sont précisés dans le document ITSB-111 (https://www.cse-cst.gc.ca/fr/node/1428/html/25015) ou dans une version ultérieure, ii) soient mises en œuvre dans un module cryptographique validé par le Programme de validation des modules cryptographiques (https://www.cse-cst.gc.ca/fr/group-groupe/programme-validation-modules-cryptographiques-pvmc), afin de respecter au minimum les exigences de validation du niveau 1 de la Federal Information Processing Standard (FIPS) 140-2, iii) fonctionnent en mode FIPS; b) l'intégrité et la confidentialité des données de la SAE durant la transmission et en période d'arrêt soient protégées à l'aide de solutions cryptographiques, sauf si elles sont protégées par d'autres mécanismes approuvés par le Canada.
E2.136	Protection du système et des communications	L'entrepreneur ne doit pas empêcher un utilisateur de chiffrer, de déchiffrer, de signer et de vérifier des fichiers en pièce jointe de la SAE à l'aide de certificats approuvés par le gouvernement du Canada.
E2.137	Protection du système et des communications	L'entrepreneur doit utiliser uniquement le code mobile approuvé au préalable dans la SAE et donc il doit refuser le téléchargement et l'exécution de tout autre code mobile.
E2.138	Protection du système et des communications	La composante ou les composantes de la SAE fournissant collectivement un service de résolution du nom ou de conversion d'adresse pour la SAE doivent effectuer une distinction des rôles internes et des rôles externes.
E2.139	Protection du système et des communications	La SAE doit permettre l'authentification de tous les types de clients logiciels à l'aide d'un justificatif de la SAE.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.140	Protection du système et des communications	La SAE doit protéger l'intégrité et la confidentialité des données de la SAE durant la transmission et en période d'arrêt à l'aide des modules et des algorithmes cryptographiques approuvés par le Centre de la sécurité des télécommunications du Canada (se reporter à la sous-section Normes de chiffrement), à moins qu'elles ne soient protégées autrement par d'autres mesures de protection physique approuvées par le Canada.
E2.141	Protection du système et des communications	L'entrepreneur peut, à sa discrétion, utiliser du matériel et des logiciels non spécialisés pour l'exploitation, l'administration et la gestion des données relatives à la SAE. L'utilisation du matériel et de logiciels non réservés n'est autorisée que pour les données de gestion de la SAE selon les conditions suivantes : a) l'accès aux données sur les utilisateurs de la SAE et le traitement ou le stockage de celles-ci sont interdits; b) l'accès aux données du système de la SAE, le traitement ou le stockage de celles-ci sont interdits; c) l'accès aux noms et aux mots de passe des comptes d'utilisateurs, et le traitement ou le stockage de ceux-ci sont interdits; d) les données doivent être séparées des autres données sur le client de manière logique; e) toutes les exigences relatives à la SAE énoncées dans l'annexe 2, Exigences en matière de sécurité, doivent être respectées; f) l'accès aux renseignements désignés protégés ou classifiés, le traitement ou le stockage de ceux-ci sont interdits, à moins que cela n'ait été approuvé par écrit par le Canada; g) l'accès aux renseignements sur l'architecture du service de la SAE, le traitement ou le stockage de ceux-ci sont interdits; h) le contrôle et la modification de la SAE réservée sont interdits.
E2.142	Protection du système et des communications	La SAE doit comprendre des contrôles spécialisés pour toute interconnexion réseau entre une SAE spécialisée ou non spécialisée, conformément à l'architecture de sécurité approuvée, qui comprend : a) la protection des limites dans lesquelles l'entrepreneur doit utiliser les pare-feu physiques actuels ou évalués précédemment (http://www.cse-cst.gc.ca/its-sti/services/cc/index-fra.html) validés à l'aide d'un schéma des Critères communs reconnu, selon un profil de protection approuvé portant sur l'évaluation des pare-feu. L'entrepreneur doit obtenir l'approbation du Canada pour l'utilisation d'un autre pare-feu physique; b) l'intégration d'un équipement de détection et de prévention des menaces fourni par l'entrepreneur; c) l'acheminement du trafic par l'intermédiaire de serveurs mandataires authentifiés; d) le contrôle de l'accès fondé sur les rôles selon le principe de droit d'accès minimal.
E2.143	Protection du système et des communications	L'entrepreneur doit physiquement ou logiquement :

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		a) séparer les renseignements qui déterminent et décrivent les incidents de sécurité de tous les autres types d'incidents. Tout renseignement sur les enquêtes liées à la sécurité généré dans le cadre du dossier doit être enregistré dans l'entreposage dédié du Canada; b) veiller à ce que tous les détails sur la configuration du réseau contenus dans les dossiers des biens et les systèmes de gestion des dossiers de configuration de l'infrastructure de la SAE soient chiffrés; c) séparer le trafic IP sur le réseau entre les données sur le système de la SAE et toutes les autres données sur la SAE; d) séparer logiquement le trafic IP sur le réseau entre les données sur la gestion de la SAE et les données sur les utilisateurs de la SAE;
E2.144	Protection du système et des communications	La catégorisation des données sur la SAE, selon qu'il s'agit de données sur le système, les utilisateurs ou la gestion de la SAE, sera à l'entière discrétion du Canada et sera fondée sur une comparaison avec d'autres données similaires
E2.145	Intégrité du système et des renseignements	L'entrepreneur doit présenter au Canada des procédures opérationnelles de sécurité relatives à la SAE qui définissent les rôles et les responsabilités opérationnels en vue de satisfaire aux exigences en matière d'intégrité du système et des renseignements énoncées dans le présent énoncé des travaux.
E2.146	Intégrité du système et des renseignements	L'entrepreneur doit définir et exécuter les processus de gestion des correctifs pour les composantes de la SAE, notamment : a) s'assurer que la version la plus récente des applications et des systèmes d'exploitation est utilisée, b) veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par le fournisseur soient appliqués rapidement; c) établir l'ordre de priorité des correctifs critiques à l'aide d'une approche fondée sur le risque; d) mettre hors ligne et remettre en ligne des applications; e) harmoniser les niveaux de criticité avec les correctifs, selon les directives du Canada; f) évaluer les vulnérabilités par rapport à la version 2 du CVSS; g) appliquer une méthodologie de mise à l'essai et de vérification pour veiller à ce que les correctifs aient été mis en œuvre de façon appropriée; h) définit les processus de gestion des correctifs pour les logiciels personnalisés utilisés dans la SAE, dont : i) la détermination, le signalement et la correction des failles dans les logiciels personnalisés, ii) la mise à l'essai des mises à jour de logiciels visant à corriger les failles afin d'en vérifier l'efficacité et les effets secondaires possibles sur la SAE avant l'installation, iii) l'intégration de correctifs des failles dans le processus de gestion de la configuration de la SAE.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.147	Intégrité du système et des renseignements	L'entrepreneur doit : a) centraliser la gestion des mécanismes de protection contre les programmes malveillants; b) mettre automatiquement à jour les mécanismes de protection contre les programmes ou les logiciels malveillants (y compris les définitions de signature) dans les six heures suivant le moment où ils sont rendus disponibles et à la demande du Canada; c) empêcher les utilisateurs non privilégiés de contourner les fonctions de protection contre les programmes malveillants; d) mettre à jour les mécanismes de protection contre les programmes malveillants uniquement à la demande d'un utilisateur privilégié; e) interdire aux utilisateurs d'introduire des supports amovibles dans la SAE.
E2.148	Intégrité du système et des renseignements	La SAE doit fournir, en priorité et dans les plus brefs délais, des alertes (p. ex. à l'aide de règles de corrélation) à la suite d'indications de compromission ou de compromission potentielle et en aviser le Canada.
E2.149	Intégrité du système et des renseignements	La SAE doit empêcher les utilisateurs non privilégiés de contourner les fonctions de détection et de prévention des intrusions.
E2.150	Intégrité du système et des renseignements	L'entrepreneur doit mettre en œuvre une solution de vérification de l'intégrité gérée de façon centralisée visant à détecter les changements non autorisés à la configuration des composantes de la SAE et des logiciels, notamment : a) effectuer des analyses de l'intégrité au moins tous les 30 jours; b) créer automatiquement un dossier d'incident de sécurité lorsque des écarts sont relevés durant une vérification de l'intégrité.
E2.151	Gestion du cycle de vie de l'information et de la sécurité des données Répertoire et flux de données	Les politiques et les procédures de la SAE doivent être établies afin de répertorier, de consigner et de tenir à jour les flux de données pour ce qui est des données qui se trouvent (de façon permanente ou temporaire) dans les applications du service et dans le réseau et les systèmes. Plus particulièrement, l'entrepreneur doit s'assurer que les données visées par des exigences relatives à leur emplacement géographique ne sont pas migrées à l'extérieur des limites définies.
E2.152	Gestion du cycle de vie de l'information et de la sécurité des données Données non liées à la production	Les données de production de la SAE ne doivent pas être reproduites ni utilisées dans des environnements de non-production.
E2.153	Chiffrement et gestion des clés Admissibilité	Les propriétaires des clés de l'infrastructure à clés publiques de la SAE doivent être identifiables (lier les clés aux identités), et des politiques de gestion des clés doivent être établies.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.154	Chiffrement et gestion des clés Génération des clés	Les politiques et les procédures opérationnelles de la SAE doivent être établies pour la gestion des clés cryptographiques dans le système cryptographique du service (p. ex. gestion du cycle de vie de la génération des clés jusqu'à la révocation et au remplacement, infrastructure à clés publiques, conception du protocole cryptographique et algorithmes utilisés, contrôles d'accès en place pour la génération sécuritaire de clés, et échange et stockage, y compris répartition des clés utilisées pour les données ou les séances chiffrées). Sur demande, l'entrepreneur doit informer le Canada des changements apportés au système cryptographique, en particulier si les données de la SAE sont utilisées dans le cadre du service ou si le client (locataire) assume une responsabilité partagée pour ce qui est de la mise en œuvre du contrôle.
E2.155	Chiffrement et gestion des clés Protection des données de nature délicate	Les politiques et les procédures opérationnelles de la SAE doivent être établies, et les processus opérationnels à l'appui ainsi que les mesures techniques doivent être mis en œuvre en vue d'utiliser des protocoles de chiffrement pour la protection des données de nature délicate stockées (p. ex. serveurs de fichiers, base de données et postes de travail des utilisateurs finaux), des données en usage (mémoire) et des données en cours de transmission (p. ex. interfaces systèmes, réseaux publics, messagerie électronique), conformément aux obligations de conformité juridiques, législatives et réglementaires.
E2.156	Chiffrement et gestion des clés Stockage et accès	Le chiffrement de la plateforme de la SAE et des données appropriées (conformément aux directives du CSTC énoncées dans le document ITSG-111 [https://www.cse-cst.gc.ca/fr/node/1428/html/25015]) dans des formats ouverts et validés et des algorithmes normalisés doit être exigé. (c.-à-d. dans le nuage de la SAE de l'entrepreneur en question); elles doivent plutôt être conservées par le Canada ou par un entrepreneur de confiance chargé de gérer les clés, selon ce qui aura été convenu mutuellement avec le Canada. La gestion et l'utilisation des clés de la SAE doivent représenter deux tâches distinctes.
E2.157	Gouvernance et gestion des risques Évaluations des risques axées sur les données	Les évaluations des risques de la SAE associées aux exigences en matière de gouvernance des données doivent être réalisées aux intervalles prévus, comme il aura été mutuellement convenu avec le Canada, et elles doivent tenir compte de ce qui suit : a) la connaissance de l'endroit où sont stockées et transmises les données de nature délicate dans les applications, les bases de données, les serveurs et le réseau; b) le respect des périodes de conservation définies et des exigences relatives à l'élimination en fin de vie; c) la classification des données et la protection de celles-ci contre l'utilisation, l'accès et la destruction non autorisés, ainsi que la perte et la falsification.
E2.158	Gouvernance et gestion des risques Surveillance de la gestion	Les gestionnaires de la SAE sont chargés de se tenir au courant des politiques, des procédures et des normes en matière de sécurité qui se rapportent à leur zone de responsabilité, et de les respecter.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.159	Gouvernance et gestion des risques Programme de gestion	L'entrepreneur doit avoir établi un programme de gestion de la sécurité de l'information, le consigner, le faire approuver et le mettre en œuvre. Ce programme doit inclure des mesures de protection administratives, techniques et physiques pour protéger les biens et les données contre la perte, l'usage abusif, ainsi que l'accès, la divulgation, l'altération et la destruction non autorisés. Le programme de sécurité doit notamment comprendre les domaines suivants, dans la mesure où ils sont liés aux caractéristiques de l'entreprise : a) gestion des risques; b) politique en matière de sécurité; c) organisation de la sécurité de l'information; d) gestion des biens; e) sécurité des ressources humaines; f) sécurité physique et environnementale; g) gestion des communications et des opérations; h) contrôle d'accès; i) acquisition, développement et maintenance de systèmes d'information.
E2.160	Gouvernance et gestion des risques Cadre de gestion des risques	Tous les risques liés à la SAE doivent être atténués à un niveau acceptable. Des niveaux d'acceptation fondés sur des critères de risque doivent être établis et consignés.
E2.161	Partitionnement des appareils interréseau des zones	L'utilisation d'appareils virtuels dans l'interréseau des zones depuis la SAE doit être suffisamment séparée des serveurs virtuels dans toutes les zones contenant des applications de la SAE.
E2.162	Partition de mémoire	La mémoire de la SAE utilisée par l'hyperviseur pour gérer les images des appareils virtuels doit être physiquement et logiquement séparée lorsque la SAE contient des applications de niveau PROTÉGÉ B pouvant causer des préjudices MOYENS, tel que défini par le Canada.
E2.163	Utilisation des caractéristiques de l'hyperviseur	Les machines virtuelles propres à l'architecture de la SAE ne doivent pas utiliser de mécanisme d'échange machine-machine (p. ex. échange de fichiers), ces derniers mécanismes étant déjà mis en œuvre par l'hyperviseur.
E2.164	Certification de l'hyperviseur	L'entrepreneur doit utiliser les hyperviseurs couramment ou précédemment évalués afin de gérer toutes les zones, tel que défini dans les directives des documents ITSG-22 (https://cse-cst.gc.ca/fr/node/268/html/15236) et ITSG-38 (https://cse-cst.gc.ca/fr/node/266/html/25034) [https://cse-cst.gc.ca/fr/group-groupe/schema-canadien-lie-aux-criteres-communs]), validés à l'aide d'un schéma lié aux Critères communs reconnus, selon un profil de protection approuvé portant sur l'évaluation des hyperviseurs pour la protection des machines virtuelles entre les zones, ou il doit obtenir l'approbation du Canada pour utiliser des produits de remplacement.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.165	Sécurité de la virtualisation Gestion des vulnérabilités	L'entrepreneur doit s'assurer que les outils ou les services d'évaluation des vulnérabilités de sécurité sont adaptés aux technologies de virtualisation utilisées (p. ex. équipement d'alerte et d'enregistrement automatiques de virtualisation) dans la SAE.
E2.166	Sécurité de la virtualisation – Environnements de production et de non-production	Les environnements de production et de non-production de la SAE doivent être séparés l'un de l'autre afin de prévenir tout accès ou changement non autorisé aux ressources d'information La séparation des environnements peut comprendre : des pare-feu à inspection dynamique, des sources d'authentification des domaines ou des partitions, et une séparation claire des tâches pour le personnel ayant accès à ces environnements dans le cadre de leurs fonctions. Ces mesures de séparation doivent recevoir l'approbation du Canada.
E2.167	Sécurité de la virtualisation – Segmentation	Les applications, le système et les composantes de réseau (physiques et virtuels) partagés par l'entrepreneur via la SAE, qu'ils soient gérés par l'entrepreneur ou lui appartiennent, doivent être conçus, développés, déployés et configurés de manière à séparer convenablement l'accès usager du fournisseur et du Canada (locataire) de celui des autres locataires utilisateurs, selon les facteurs suivants : a) les politiques et les procédures établies; b) l'isolement des biens essentiels aux opérations et des données de nature délicate sur les utilisateurs, qui exigent des contrôles internes renforcés et des niveaux d'assurance élevés; c) le respect des obligations de conformité juridiques, législatives et réglementaires applicables.
E2.168	Interopérabilité et portabilité Virtualisation	L'entrepreneur doit utiliser une plateforme de virtualisation reconnue par l'industrie et des formats de virtualisation normalisés (p. ex. OVF) pour assurer l'interopérabilité. L'entrepreneur doit aussi consigner les changements personnalisés apportés aux hyperviseurs en utilisation et à tous les crochets de virtualisation propres à la SAE qui sont disponibles aux fins des examens réalisés par le Canada.
E2.169	Évaluation des facteurs relatifs à la vie privée	À la demande du Canada, l'entrepreneur doit participer activement à la réalisation d'une évaluation des facteurs relatifs à la vie privée de la SAE, conformément à la Politique sur la protection de la vie privée du SCT du Trésor (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12510).
E2.170	Protection physique et environnementale	L'entrepreneur doit : a) mener une enquête sur les personnes avant de leur donner accès au système d'information, conformément à la *Norme sur la sécurité du personnel du SCT*; b) mener une deuxième enquête sur les personnes si les conditions définies à cet égard sont remplies; c) dans le cas des entrepreneurs étrangers, consulter la partie 6, 6.1 (a) – Exigences en matière de sécurité et de protection des renseignements personnels pour les entrepreneurs étrangers (filtrage de sécurité du personnel).

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
E2.171	Protection physique et environnementale	L'entrepreneur doit : a) respecter les exigences de contrôle de la sécurité du personnel, incluant les rôles et les responsabilités des fournisseurs tiers; b) consigner les exigences de contrôle de la sécurité du personnel; c) surveiller la conformité des fournisseurs; d) veiller à ce que les organisations et les personnes du secteur privé qui ont accès à des renseignements et à des biens protégés fassent l'objet d'une enquête de sécurité; e) définir explicitement la surveillance gouvernementale ainsi que les rôles et les responsabilités des utilisateurs finaux relativement aux services fournis par des tiers.
E2.172	Protection physique et environnementale	a) L'entrepreneur est responsable du recrutement du personnel. b) L'entrepreneur doit : • tenir à jour une liste des employés indiquant clairement leur nom, leur titre, leurs responsabilités, les formations qu'ils ont suivies, et leurs niveaux d'accès aux installations et aux systèmes, conformément aux exigences énoncées dans l'énoncé des besoins; • fournir la liste aux dirigeants du projet de la SPAC, à la demande de ces derniers; • maintenir un dossier qui démontre que les employés de l'entrepreneur possèdent les compétences nécessaires à la réalisation des travaux. Ce dossier doit être fourni aux dirigeants du projet de la SPAC à la demande de ces derniers; • durant la période visée par le contrat, fournir aux dirigeants du projet de la SPAC, sur demande, un rapport de vérification du casier judiciaire et de vérification de la solvabilité pour tout employé, à la discrétion de l'autorité contractante; • conserver la documentation sur les enquêtes de sécurité dans un dossier accessible à l'autorité contractante pour chaque employé pendant une période de dix ans suivant l'offre d'emploi initiale; • mener une deuxième enquête sur les personnes si les conditions le justifient.
E2.173	Sécurité opérationnelle	L'entrepreneur doit : a) s'assurer que toutes les activités réalisées relativement aux exigences de sécurité et de protection des renseignements personnels dans l'énoncé des travaux fournissent des niveaux de protection similaires à ceux définis dans les politiques du gouvernement du Canada et respectent ou surpassent les pratiques exemplaires ou les normes de l'industrie (p. ex. ISO 27001), les exigences les plus rigoureuses étant retenues; b) à la demande de l'autorité contractante, fournir une preuve de conformité avec les lois du pays dans lequel les activités sont réalisées, ce qui peut notamment comprendre la conformité avec les lois nationales concernant la protection des renseignements personnels, les lois fiscales, les règlements constitutifs et les lois sur le travail;

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Description
		c) désigner un agent de sécurité d'entreprise autorisé qui sera chargé de surveiller l'application des exigences en matière de sécurité et de protection des renseignements personnels traités dans le cadre du contrat. Cet agent servira de point de contact pour les questions relatives à la protection des renseignements personnels et à la sécurité, en collaboration avec l'autorité contractante. L'agent de sécurité d'entreprise collaborera avec l'autorité contractante dans le traitement des demandes d'accès à l'information et de la protection des renseignements personnels. L'agent sera aussi chargé de surveiller l'application des pratiques relatives à la sécurité et à la protection des renseignements personnels et de répondre aux commentaires provenant d'audits. De plus amples renseignements sur la désignation et les responsabilités de l'agent de sécurité d'entreprise sont disponibles à l'adresse suivante : http://ssi-iss.tpsgc-pwgsc.gc.ca/msi-ism/ch1-fra.html#ch1-103; d) désigner une personne-ressource principale responsable de la sécurité de la TI. Cette personne-ressource, qui doit entretenir une relation hiérarchique fonctionnelle avec la Gestion de la sécurité, sera chargée d'assurer l'exécution des activités suivantes : i. mettre en place et gérer le programme de sécurité de la TI de l'entrepreneur dans le cadre d'une approche de sécurité globale; ii. cerner, définir et consigner les rôles et les responsabilités relatifs à la sécurité du système d'information; iii. formuler des recommandations concernant l'approbation de tous les contrats liés à des fournisseurs externes de services de sécurité de la TI; iv. collaborer avec les gestionnaires responsables de la réalisation des programmes et de la prestation des services afin d'assurer la satisfaction de leurs besoins en matière de sécurité de la TI et fournir des conseils sur les mesures de protection, les répercussions éventuelles de menaces nouvelles ou existantes et le risque résiduel d'un programme ou d'un service; v. surveiller la conformité ministérielle avec les normes en matière de sécurité; vi. établir un processus efficace de gestion des incidents de sécurité liés à la TI, et surveiller la conformité.

SECTION II – EXEMPLE DE MATRICE DE TRAÇABILITÉ DES EXIGENCES RELATIVES À LA SÉCURITÉ

Le **Tableau 2** ci-dessous est un exemple de matrice de traçabilité des exigences relatives à la sécurité.

Nº d'id. de la section de la DP pour la SAE	Catégorie de l'exigence	Énoncé de l'exigence	Renvoi à l'énoncé des travaux	Méthode d'évaluation	Critères d'évaluation	Points de contrôle du processus d'évaluation et d'autorisation de sécurité		
						Point de contrôle 1 – Traçabilité des spécifications de sécurité générales de l'architecture des services (conformité avec l'exigence)	Point de contrôle 2 – Traçabilité des spécifications de sécurité détaillées de l'architecture des services (conformité avec l'exigence)	Point de contrôle 3 – Traçabilité de la vérification et de la validation de l'intégration (conformité avec l'exigence)
E2.1	Contrôle de l'accès	L'entrepreneur doit : a) élaborer, diffuser, examiner et mettre à jour chaque année les politiques sur le contrôle d'accès et les exigences connexes en matière de contrôle d'accès pour les composantes de la SAE; b) fournir au gouvernement du Canada les procédures de sécurité opérationnelles qui définissent les rôles opérationnels et les responsabilités en matière de contrôle d'accès.						
E2.2	Contrôle de l'accès	Les services de GIJIA doivent créer automatiquement des comptes d'utilisateur et des comptes génériques pour la SAE, c'est-à-dire : a) attribuer un compte et un nom d'affichage uniques pour la SAE, conformément à la norme définie dans l'Énoncé des travaux, en appliquant les règles configurables de résolution de conflits et de désignation; b) créer un compte sans privilège; c) attribuer un mot de passe temporaire applicable au compte; d) établir les attributs du compte et les privilèges de sécurité d'accès selon les directives du gouvernement du Canada; e) communiquer le compte, le nom d'affichage et le mot de passe unique attribués pour la SAE au demandeur du compte.						