Produits d’impression pour ATMT
Exigences en matière de sécurité
Appendice G

1 ENTENTES D'ACCÈS *(AMF ET SGI)*

L'entrepreneur doit conclure des ententes d'accès aux SGI dans les cas suivants :

a. avant de se voir accorder un accès aux SGI ou aux données, les administrateurs 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 doit examiner et mettre à jour les ententes d'accès aux SGI ou aux données sur une base annuelle.

L'entrepreneur doit utiliser un processus formel de sanctions pour le personnel qui ne se conforme pas aux politiques et procédures établies de sécurité de l'information.

L'entrepreneur doit rendre facilement accessibles les règles qui décrivent les responsabilités et le comportement attendu des personnes qui doivent accéder au système d'information concernant l'utilisation de l'information et du système d'information. Les règles relatives au comportement doivent être fondées sur les rôles et responsabilités de chaque utilisateur, en distinguant, par exemple, les règles qui s'appliquent aux utilisateurs privilégiés et les règles qui s'appliquent aux utilisateurs généraux.

2 CONTRÔLE D'ACCÈS À L'INFRASTRUCTURE *(SGI)*

Tous les terminaux du SGI, y compris les appareils mobiles, doivent être gérés par le GC ou par l'entrepreneur.

L'entrepreneur doit mettre en œuvre toutes les mesures appropriées pour éviter que le réseau du GC ne soit relié à des services sans fil externes.

3 CONTRÔLE DE L'ACCÈS AUX MOYENS DE TRANSMISSION *(SGI)*

L'entrepreneur doit :

a. contrôler l'accès physique au portail de prestation de services pour le SGI et aux lignes de distribution à l'intérieur des installations du fournisseur;
b. protéger l'équipement de télécommunications, le câblage et les relais qui transmettent les données du SGI ou qui appuient les services contre les interceptions ou les dommages et intégrer à leur conception des redondances et des sources d'alimentation et voies d'acheminement de rechange;
c. protéger le câblage des télécommunications de l'interception non autorisée et contre les dommages;
d. contrôler l'accès au câblage, aux espaces et aux chemins d'accès de télécommunication (p. ex. les salles de télécommunications, les salles de l'ordinateur central et les autres salles contenant du matériel).

4 POLITIQUES ET PROCÉDURES DE CONTRÔLE D'ACCÈS *(SGI)*

L'entrepreneur doit démontrer que les politiques de contrôle d'accès et les exigences connexes en matière de contrôle d'accès sont en place pour les composantes du Service de gestion d'impression (SGI).

L'entrepreneur doit démontrer que les procédures actuelles de gestion des comptes des ressources et du personnel de l'entrepreneur pour les composantes du SGI sont en place.

5 APPLICATION DE L'ACCÈS

Le SGI ne doit permettre un accès logique au système, aux applications, aux appareils, aux fichiers, aux données pertinentes pour la sécurité et aux autres ressources qu'aux entités autorisées (utilisateurs ou processus), conformément aux politiques de contrôle d'accès applicables. Le contrôle de l'accès doit être conforme à la Norme sur la gestion du contrôle d'accès logique de SPC (http://service.ssc-spc.gc.ca/fr/politiques_processus/politiques/logique-v2). ***(AMF et SGI)***

L'entrepreneur doit mettre en œuvre toutes les mesures appropriées pour prévenir une atteinte à la protection des données et ne doit pas accorder l'accès à des renseignements ou à des données liées au GC ou propres au GC sans l'autorisation écrite de SPC ou du ministère ou organisme.

L'entrepreneur doit immédiatement aviser par écrit SPC ou le ministère ou organisme de tout accès non autorisé, réel ou soupçonné, aux systèmes, données, renseignements ou infrastructures du GC.

6 RESTRICTIONS D'ACCÈS CONCERNANT LES CHANGEMENTS *(SGI)*

L'entrepreneur ne doit permettre un accès aux systèmes d'information qu'aux personnes qualifiées et autorisées aux fins de mise en œuvre des changements approuvés par SPC ou par le ministère ou organisme, y compris les mises à niveau et les modifications.

L'entrepreneur doit tenir des registres d'accès pour s'assurer que les contrôles des changements de configuration sont mis en œuvre et pour appuyer les mesures prises après coup si SPC, le ministère, l'organisme ou l'entrepreneur découvrent des changements non autorisés.

Le SGI doit faire respecter les restrictions d'accès liées aux modifications du système et appuyer la vérification des mesures d'application.

L'entrepreneur doit passer en revue les changements apportés au système d'information chaque trimestre pour déterminer si des changements non autorisés ont été apportés.

7 GESTION DES COMPTES

Le SGI doit fermer la session des utilisateurs après une période d'inactivité déterminée par SPC ou par le ministère ou organisme. La durée de cette période doit être configurable. ***(SGI)***

Le SGI doit fermer la session des utilisateurs privilégiés (administrateurs de l'entrepreneur et administrateurs du GC) après une période d'inactivité déterminée par SPC ou par le ministère ou organisme. ***(AMF et SGI)***

L'entrepreneur doit gérer les comptes d'opérateurs, d'administrateurs et d'utilisateurs privilégiés du SGI des façons suivantes :

a. créer et gérer tous les types de comptes conformément à des profils d'accès basés sur des rôles qui précisent les privilèges ***(AMF et SGI);***
b. assurer que les appareils multifonctions (AMF) ont la capacité d'assigner aux utilisateurs des rôles qui distinguent les utilisateurs qui peuvent exécuter des fonctions administratives des utilisateurs qui exécutent des fonctions non privilégiées ***(AMF);***
c. surveiller et faire le suivi de l'attribution des rôles d'opérateur, d'administrateur et d'utilisateur ***(SGI)***;
d. ajuster l'attribution des rôles d'opérateur, d'administrateur et d'utilisateur par des changements de rôle ***(SGI).***

8 PARTITIONNEMENT DES APPLICATIONS *(AMF ET SGI)*

Le SGI et les appareils d'impression doivent :

a. Séparer les fonctions destinées aux utilisateurs (y compris les services de l'interface utilisateur) des fonctions de gestion de l'infrastructure;
b. Empêcher l'affichage des fonctions liées à la gestion de l'infrastructure dans l'interface destinée aux utilisateurs ordinaires (sans privilèges).

Le portail de prestation de services, le SGI et les appareils d'impression doivent isoler les fonctions de gestion et de sécurité des utilisateurs non privilégiés et des fonctions qui ne sont pas liées à la sécurité. Par exemple, ces fonctions peuvent être utilisées à partir d'ordinateurs différents, d'unités centrales différentes, d'instances de systèmes d'exploitation différentes, d'adresses réseau différentes, avec des techniques de virtualisation ou avec une combinaison de ces méthodes ou d'autres, selon le cas. Ce type de séparation comprend, par exemple, des interfaces administratives en ligne qui utilisent des méthodes d'authentification distinctes (p. ex. en utilisant une séparation logique, les administrateurs Web utilisent une authentification à deux facteurs et les utilisateurs normaux de l'application Web, une authentification par nom d'utilisateur et mot de passe). La séparation des fonctions du système et de l'utilisateur peut inclure l'isolement des interfaces d'administration sur différents domaines et avec des contrôles d'accès supplémentaires.

9 EXAMEN ET ANALYSE DES VÉRIFICATIONS ET PRODUCTION DES RAPPORTS CONNEXES *(SGI)*

L'entrepreneur doit mettre en œuvre un processus d'examen de vérification qui comprend ce qui suit :

a. définition du niveau de vérification et établissement du personnel responsable de l'examen des registres de vérification;
b. examen et analyse des dossiers de vérification du SGI, chaque année et sur demande de SPC ou du ministère ou organisme, en cas de signes d'activité inappropriée ou inhabituelle, dans un délai convenu en JOGF;
c. communication des conclusions de l'examen des dossiers de vérification à SPC, dans le nombre de JOGF convenu après la fin des vérifications;
d. ajustement du niveau d'examen et d'analyse des vérifications, ainsi que du niveau des rapports subséquents, lorsque les risques changent ou sur demande de SPC.

10 ÉVÉNEMENTS VÉRIFIABLES

Le SGI doit consigner toutes les communications pour chaque travail d'impression, notamment les communications suivantes, telles qu'approuvées par SPC ou par le ministère ou organisme ***(SGI)*** :

a. date et heure du travail d'impression;
b. adresse IP de l'expéditeur;
c. adresse IP de l'imprimante destinataire;
d. nom d'hôte d'envoi;
e. utilisation du protocole de sécurité de la couche transport (TLS);
f. ID du travail d'impression;
g. nom d'utilisateur.

Le SGI et le portail de prestation de services doivent au moins consigner et vérifier les événements d'utilisateur ou de processus privilégiés suivants. Toute exception doit être approuvée par le GC ***(AMF et SGI) :***

a. Tentatives fructueuses et infructueuses d'accès, de modification ou de suppression d'objets de sécurité (ces objets incluent les données de vérification, les fichiers de configuration de système et les permissions d'accès formelles d'utilisateur)
b. Tentatives fructueuses et infructueuses de connexion
c. Activités privilégiées
d. Heure de début de l'accès de l'utilisateur au système
e. Tous les lancements de programme

De plus, le système d'information doit vérifier au moins les événements d'utilisateur ou de processus non privilégiés suivants : toute exception doit être approuvée par le GC ***(AMF et SGI)*** :

a. Tentatives fructueuses et infructueuses d'accès, de modification ou de suppression d'objets de sécurité
b. Tentatives fructueuses et infructueuses de connexion
c. Heure de début de l'accès de l'utilisateur au système
d. Informations sur l'IP de la source

L'entrepreneur doit informer SPC ou le ministère ou organisme des nouveaux événements vérifiables et coordonner le processus de vérification pour l'enregistrement des nouveaux événements. ***(AMF et SGI)***

11 RÉTROACTION D'AUTHENTIFICATION *(AMF ET SGI)*

Les composants du SGI et les appareils d'impression doivent masquer la rétroaction des données d'authentification (p. ex. masquer les champs de mot de passe) pendant le processus d'authentification afin de protéger les renseignements d'une exploitation/utilisation possible par des personnes non autorisées.

12 CONFIGURATION *DE BASE (SGI)*

L'entrepreneur doit présenter la configuration de base actuelle des composants du SGI. Les configurations de base comprennent des informations sur les composants du système d'information (p. ex. les progiciels standard installés sur les serveurs, les composants du réseau ou les appareils mobiles; les numéros des versions actuelles et les renseignements sur les correctifs des systèmes d'exploitation et des applications; les paramètres de configuration), la topologie du réseau et le placement logique de ces composants dans l'architecture de système. La configuration de base doit également démontrer que tous les ports, services et logiciels inutilisés ont été désactivés et utilisent une configuration à sécurité renforcée (p. ex. comptes invités désactivés, contrôle d'accès appliqués à tous les fichiers et répertoires système, mots de passe par défaut modifiés). Le système d'exploitation du portail de prestation de services de l'entrepreneur est également considéré comme un élément de configuration.

L'entrepreneur doit examiner et mettre à jour la configuration de base du SGI :

a. au besoin, en raison d'un incident ou d'un changement d'élément de configuration;
b. dans le cadre du processus d'installation et de mise à niveau des composants du SGI.

Afin de limiter les exploits potentiels, l'identifiant et le mot de passe administrateur par défaut du service et de l'appareil doivent être modifiés avec des mots de passe complexes lors de la configuration initiale et de l'installation. ***(AMF et SGI)***

13 PROTECTION DES LIMITES *(SGI)*

L'entrepreneur doit placer le portail de prestation de services pour les composantes matérielles du SGI et les biens connexes dans un endroit sûr. La zone sécurisée doit être dotée de contrôles de sécurité physiques permettant l'accès uniquement au personnel autorisé de l'entrepreneur.

14 CRITÈRES COMMUNS *(AMF)*

Le profil de protection des critères communs « Protection Profile for Hardcopy Devices » (version 1.0, 10 septembre 2015, Information-technology Promotion Agency [IPA], National Information Assurance Partnership [NIAP] et la communauté technique des AMF) doit être appliqué lors de l'achat de nouveaux appareils multifonctions. Les appareils multifonctions doivent être certifiés conformément au profil de protection des dispositifs de copie. Les principaux éléments des annexes du profil de protection doivent être utilisés pour les tests et évaluations de la sécurité au cours du processus d'évaluation de la sécurité et d'autorisation, car les cas de tests fournis permettront de recueillir des éléments aux fins d'examen.

Le Canada comprend que l'industrie est encore en cours de transition vers une certification HCDPP; par conséquent, l'offrant doit fournir des AMF certifiés conformément à la documentation HCDPP de 2015 en date du 31 août 2019. Après le 31 août 2019, seuls les AMF conformes à HCDPP seront acceptés.

Avant le 31 août 2019,

1. Le Canada étendra son acceptation aux appareils qui sont en voie d'être certifiés HCDPP, mais qui n'ont pas encore fait l'objet d'une évaluation exhaustive, à condition qu'un examen plus approfondi soit effectué pour valider la pleine conformité à HCDPP.
2. Le Canada autorisera les dispositifs avec la norme IEEE 2600.2 à condition que l'offrant démontre que les aspects clés suivants en matière de sécurité sont conformes à l'aide des cas de test fournis dans les annexes de l'HCDPP ou au moyen d'un plan de test et d'une attestation acceptés par le GC :
    a. Les éléments de sécurité des télécopieurs doivent démontrer qu'il n'est pas possible d'établir une passerelle avec le réseau;
    b. La capacité de réécriture des transactions individuelles doit être la même que les niveaux d'HCDPP;
    c. Le chiffrement est limité à des niveaux de chiffrement précis et tous ces niveaux respectent les forces approuvées par le Centre de la sécurité des télécommunications. Les autres stratégies de chiffrement ne seront pas considérées comme acceptables;
    d. Veiller à ce que des exigences spécifiques concernant les communications sécurisées (TLS/HTTPS/IPSEC/SSH) soient en place;

e. S'assurer que l'entropie fournie pour le processus de génération des clés est suffisante et justifiée conformément à HCDPP (appendice E);
f. S'assurer que les détails concernant la gestion des clés sont documentés et présentés conformément à HCDPP (appendice F);
g. S'assurer que la fonction de remise à zéro des clés soit disponible et activée;
h. Fournir l'assurance des capacités de contrôle d'accès basé sur les rôles (RBAC) des appareils afin de démontrer la séparation en ce qui a trait la configuration des appareils entre le mode technicien ou de réparation et la configuration des comptes et des données traitées;
i. Tout autre critère du profil de protection HCDPP si le GC en fait la demande.

15 CONTRÔLE DES CHANGEMENTS DE CONFIGURATION *(SGI)*

L'entrepreneur doit appuyer les processus de gestion de la configuration du SGI, notamment par les moyens suivants :

a. déterminer les types de changement contrôlés au moyen de la configuration;
b. approuver les changements contrôlés au moyen de la configuration en tenant explicitement compte des analyses des répercussions sur la sécurité;
c. consigner les changements contrôlés au moyen de la configuration qui sont approuvés;
d. conserver et examiner les enregistrements des changements contrôlés au moyen de la configuration;
e. vérifier les activités associées aux changements contrôlés au moyen de la configuration;
f. élaborer des procédures de distribution, d'installation et d'annulation des changements apportés en vue du lancement d'une version du SGI;
g. tester les logiciels et le matériel nouveaux et modifiés sans utiliser l'environnement de production.

16 PLAN DE GESTION DE LA CONFIGURATION *(SGI)*

L'entrepreneur doit présenter un plan de gestion de la configuration qui :

a. décrit les processus et procédures de gestion de la configuration et les rôles et responsabilités en la matière;
b. définit les éléments de configuration du SGI et le moment où ces éléments sont soumis au processus de gestion de la configuration;
c. définit les modes d'identification des éléments de configuration à employer tout au long du cycle de développement des systèmes ainsi que le processus de gestion de la configuration de ces éléments;
d. définit une capacité de protection contre les logiciels malveillants (antivirus) pour :
    i. mettre automatiquement à jour les mécanismes de protection contre les programmes malveillants, y compris les définitions des signatures;
    ii. effectuer des analyses de l'infrastructure (serveurs, ordinateurs de bureau et portables);
    iii. mettre en quarantaine les programmes malveillants détectés.
e. définit les processus de gestion des correctifs pour le SGI, dont :

i) s'assurer que les versions les plus appropriées du micrologiciel, des applications et des systèmes d'exploitation sont utilisées, conformément à la dernière évaluation des risques;

ii) veiller à ce que les vulnérabilités soient évaluées et à ce que les correctifs de sécurité fournis par l'entrepreneur soient appliqués rapidement;

iii) établir l'ordre de priorité des correctifs critiques à l'aide d'une approche fondée sur le risque; v) harmoniser les niveaux d'importance des correctifs selon les directives de SPC ou du ministère ou organisme;

iv) attribuer une cote aux vulnérabilités qui s'appuie sur la deuxième version du Common Vulnerability Scoring System (CVSS);

v) appliquer une méthodologie de mise à l'essai et de vérification pour s'assurer que les correctifs ont été mis en œuvre correctement;

vi) aviser SPC ou le ministère ou organisme des vulnérabilités liées à la configuration qui permettraient à une personne non autorisée de compromettre la confidentialité, l'intégrité ou la disponibilité du SGI.

Le plan de gestion du changement du SGI doit au moins contenir les renseignements suivants :

a. les pouvoirs de l'entrepreneur en matière de gestion du changement;
b. les rôles et responsabilités des employés de l'entrepreneur;
c. la façon dont il utilisera le processus de gestion des changements afin de soutenir le développement des services de TI du SGI (p. ex. le concept d'opération);
d. la méthode d'identification unique des éléments de configuration;
e. l'identification des éléments de la configuration;
f. la description du processus de gestion du changement, y compris le processus d'examen et d'approbation du changement;
g. les mesures mises en œuvre pour n'appliquer que les changements autorisés;
h. les procédures qu'utilisera l'entrepreneur pour accepter les éléments de configuration modifiés ou nouvellement créés.

17 POLITIQUE ET PROCÉDURES RÉGISSANT LA GESTION DE LA CONFIGURATION (SGI)

L'entrepreneur doit démontrer aux ministères et organismes ou à SPC qu'il peut assurer la prestation de ce qui suit :

a. une politique de gestion des configurations qui définit l'objectif, la portée, les rôles, les responsabilités, l'engagement de la direction, la coordination entre les entités organisationnelles et le respect;
b. des procédures visant à faciliter la mise en place de la politique de gestion des configurations et les contrôles connexes.

18 PARAMÈTRES DE CONFIGURATION *(SGI)*

L'entrepreneur doit gérer les paramètres de configuration du SGI, notamment :

a. préciser les paramètres de configuration à utiliser afin d'accorder les droits d'accès minimaux;
b. consigner les exceptions aux paramètres de configuration;

c. surveiller et contrôler les modifications apportées aux paramètres de configuration conformément aux processus de gestion des changements et de la configuration.

19 CONTENU DES DOSSIERS DE VÉRIFICATION *(AMF ET SGI)*

Les dossiers de vérification des appareils d'impression et du SGI (y compris le portail de prestation de services) doivent inclure les événements consignés suivants, à moins d'approbation contraire de SPC ou du ministère ou organisme :

a. le type d'événement de vérification qui s'est produit;
b. le moment où l'événement de vérification s'est produit (date et heure);
c. l'emplacement de l'événement de vérification;
d. la source de vérification de l'événement;
e. le résultat de l'événement de vérification (réussite ou échec);
f. l'identité de tout utilisateur ou sujet lié à l'événement de vérification;

L'entrepreneur doit travailler avec SPC ou avec le ministère ou l'organisme pour déterminer quels autres événements de vérification pourraient être requis à l'avenir.

Le SGI et les AMF doivent pouvoir gérer la capacité de stockage des dossiers de vérification par les moyens suivants :

a. conserver trois mois d'événements et d'enregistrements en ligne;
b. conserver les événements et les journaux associés à un incident de sécurité pendant au moins deux ans;
c. accorder une capacité de stockage suffisante pour les dossiers de vérification;
d. configurer la vérification de manière à empêcher le dépassement de la capacité de stockage;
e. alerter l'opérateur lorsque le volume de stockage des dossiers de vérification atteint 75 % de la capacité de stockage;
f. écraser les dossiers de vérification les plus anciens si la capacité maximale de stockage est atteinte.

Le SGI et les appareils multifonctions dans les locaux du GC doivent permettre de décharger en temps réel les dossiers de vérification vers un système de vérification et de journalisation appartenant à SPC ou aux ministères et organismes. Cette capacité doit inclure la capacité de transmettre en toute sécurité les journaux d'audit en temps quasi réel à un système central de journalisation (p. ex. le système de gestion de l'information et des événements de sécurité de SPC); SPC et l'entrepreneur conviendront du format utilisé et du contenu. Cette fonctionnalité doit être mise en œuvre par l'entrepreneur dans les 60 jours ouvrables du gouvernement fédéral suivant la demande de SPC et doit pouvoir protéger les renseignements consignés dans le registre contre toute divulgation ou modification non autorisée pendant le transfert vers le système central de journalisation.

20 PLAN D'URGENCE *(SGI)*

L'entrepreneur doit démontrer qu'il est en mesure d'offrir un plan de continuité des services pour le SGI installé dans les locaux du GC, qui est coordonné et communiqué avec le personnel participant au soutien du plan, et qui doit au minimum :

a. établir un plan détaillé et des processus consignés pour la restauration du service du SGI;

b. décrire 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;
c. planifier le transfert des fonctions d'exploitation, de gestion et d'administration à un centre des opérations secondaire;
d. planifier la reprise des missions et fonctions opérationnelles essentielles dans un délai convenu, comme approuvé par SPC ou par le ministère ou organisme;
e. énoncer les objectifs de rétablissement, les priorités de restauration, ainsi que les mesures;
f. décrire les rôles et les responsabilités ainsi que les coordonnées de chacune des personnes chargées d'intervenir en cas d'urgence;
g. décrire les mesures qui seront prises pour rétablir complètement le système d'information sans nuire aux mesures de sécurité prévues à l'origine et mises en œuvre;
h. décrire la planification de la capacité nécessaire pour assurer le traitement des données, les télécommunications et le soutien des environnements d'exploitation pendant les opérations d'urgence;
i. décrire le processus de haut niveau pour tester le plan de continuité;
j. être passé en revue et approuvé par le GC tous les ans.

21 MAINTENANCE DIRIGÉE *(SGI)*

L'entrepreneur doit effectuer une maintenance dirigée :

a. en planifiant, en exécutant et en consignant la maintenance et les réparations des composantes du SGI conformément aux spécifications du fabricant ou de l'entrepreneur, et en examinant les dossiers de maintenance;
b. en supervisant toutes les activités de maintenance, qu'elles soient exécutées sur les lieux ou à distance et que l'équipement soit entretenu sur les lieux ou dans un autre emplacement;
c. en demandant l'autorisation explicite d'un agent autorisé du GC désigné pour retirer certaines composantes du SGI du point de prestation de services de l'entrepreneur aux fins de maintenance ou de réparations hors site;
d. en s'assurant que l'équipement et les supports d'information connexes sont nettoyés (les données sont supprimées de façon permanente et ne peuvent être récupérées), comme approuvé par SPC ou par le ministère ou organisme avant leur retrait des installations de l'organisation;
e. en vérifiant 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.

22 GESTION DES JUSTIFICATIFS D'IDENTITÉ

L'accès au portail de prestation de services doit être sécurisé pour les utilisateurs finaux autorisés.

L'entrepreneur doit fournir et gérer les justificatifs d'identité (authentifiants) pour l'accès du personnel de l'utilisateur final et de l'entrepreneur au portail de prestation de services. L'entrepreneur doit également :

a. gérer les authentifiants du système d'information en vérifiant, au moment de la distribution initiale d'un authentifiant, l'identité de la personne, le groupe, le rôle ou le dispositif recevant l'authentifiant;

b. gérer les authentifiants du système d'information en établissant le contenu initial des authentifiants;
c. gérer les authentifiants en s'assurant que le mécanisme d'authentification est suffisamment robuste pour l'utilisation prévue;
d. gérer les authentifiants du système d'information en établissant et en mettant en application des procédures administratives concernant la distribution initiale des authentifiants, les authentifiants perdus, endommagés ou compromis, et l'annulation des authentifiants;
e. gérer les authentifiants du système d'information en modifiant le contenu par défaut des authentifiants avant l'installation du système d'information;
f. gérer les authentifiants du système d'information en établissant les restrictions minimales et maximales de durée et les conditions de réutilisation des authentifiants;
g. gérer les authentifiants du système d'information en modifiant ou en rafraîchissant les authentifiants après une période de temps définie pour chaque type d'authentifiant;
h. gérer les authentifiants du système d'information en protégeant le contenu des authentifiants contre toute divulgation ou modification non autorisée;
i. gérer les authentifiants des systèmes d'information en exigeant que les individus mettent en place des mesures de sécurité spécifiques pour protéger les authentifiants;
j. gérer les authentifiants du système d'information en modifiant les authentifiants pour les comptes de groupes ou de rôles lorsque le statut de membre de ces groupes ou rôles des employés de l'entrepreneur change;
k. ne pas permettre l'intégration d'authentifiants statiques non chiffrés dans les systèmes, les applications, les scripts d'accès ou les touches de fonction.

23 AUTHENTIFICATION PAR MODULE CRYPTOGRAPHIQUE *(AMF ET SGI)*

Toute utilisation de modules cryptographiques pour l'authentification auprès du SGI ou des appareils multifonctions doit utiliser une cryptographie approuvée par le CST (https://www.cse-cst.gc.ca/fr/node/1831/html/26515).

24 SUPPRESSION DES DONNÉES *(SGI)*

L'entrepreneur doit supprimer de façon permanente les données du SGI spécifiées, à la demande de SPC ou du ministère ou organisme, conformément aux lignes directrices approuvées par le CST (par exemple le document ITSG-06). L'entrepreneur doit également fournir à SPC ou au ministère ou organisme la preuve (comme un certificat de destruction) que les données du SGI indiquées ont été supprimées.

25 PROTECTION DES DONNÉES *(SGI)*

Les données du système et les données utilisateur doivent demeurer dans les locaux du GC et ne peuvent être stockées ou consultées à l'extérieur du GC à moins d'avoir obtenu l'approbation par écrit de SPC ou du ministère ou de l'organisme.

L'entrepreneur peut utiliser ses propres installations externes pour les données de gestion des services, conformément aux conditions suivantes et avec approbation de SPC ou du ministère ou de

l'organisme :

a. doivent être séparées (logiquement ou physiquement) des données des autres clients qui ne font pas partie du gouvernement du Canada. La méthode pour séparer les données du GC des données des autres clients doit être déterminée par l'entrepreneur;
b. ne doivent pas contenir de renseignements « Protégé B » ou « Classifié ».

Veuillez consulter les définitions relatives à cette exigence ci-dessous :

Les **données du système** sont les données que l'entrepreneur utilise pour contrôler ou modifier le fonctionnement, l'administration et la gestion de la solution de gestion d'impression et de la solution de gestion des appareils, y compris l'information sur :

a) les incidents de sécurité et les alarmes et événements liés à la sécurité;

b) la gestion de l'information et des événements de sécurité;

c) la gestion du périmètre du réseau (p. ex. pare-feu);

d) la gestion des intrusions et de la prévention;

e) la protection contre les logiciels malveillants et les contrôles de sécurité;

f) la gestion de l'hyperviseur et des systèmes de la machine virtuelle;

g) la gestion du réseau et les opérations;

h) les fichiers, les registres et les scripts relatifs à la configuration du système;

i) les systèmes d'authentification, d'autorisation et de comptabilité;

j) les systèmes à disques;

k) les systèmes de gestion des ressources et de la capacité;

l) la distribution, les mises à jour et les correctifs des logiciels;

m) les services d'annuaire.

Les **données d'utilisateur** sont les données relatives aux documents et dossiers d'utilisateur qui sont numérisés, télécopiés et imprimés, ainsi que les données de compte et de répertoire connexes de l'utilisateur.

Les **données de gestion des services** sont les données issues de l'exploitation, de l'administration et de la gestion des services de soutien et de la facturation :

a) les demandes de service;

b) les dossiers d'incident (à l'exception des dossiers d'incident de sécurité);

c) les documents de facturation et les factures à l'échelle de l'organisation;

d) les dossiers sur les biens;

e) les dossiers sur la configuration;

f) les données sur la performance du système, la capacité et la planification des ressources;

g) des détails sur l'état des appareils, les codes d'erreur et les événements.

26 SOUVERAINETÉ DES DONNÉES *(SGI)*

Tous les composants du SGI, les renseignements protégés et classifiés ainsi que les renseignements indiqués par SPC ou par le ministère ou organisme doivent être situés dans les limites géographiques du Canada, y compris les consulats et ambassades du Canada à l'étranger. L'approbation du GC est requise pour pouvoir transférer de l'information à l'extérieur du Canada; un tel transfert doit utiliser les formats convenus préalablement.

a. Tous les SGI et dépôts de données contenant des renseignements protégés ou classifiés doivent être conservés dans les limites géographiques du Canada, y compris les consulats et ambassades du Canada à l'étranger;
b. Les entrepôts d'objets média utilisés pour la sauvegarde, la récupération des données, l'archivage historique ou à d'autres fins doivent être hébergés dans des endroits sécurisés et approuvés à l'intérieur des frontières géographiques du Canada;
c. Toutes les données d'impression et toutes les communications avec les appareils multifonctions du GC situés au Canada ou à l'étranger (c.-à-d. les consulats et ambassades du Canada) doivent passer par des réseaux protégés adéquats. Les données en transit ne doivent pas être sauvegardées/stockées de leur point de départ à leur point d'arrivée;
d. SPC et le ministère ou l'organisme entendent s'assurer qu'il n'existe pas d'accès non autorisés aux données du GC (c'est-à-dire que l'accès n'a pas été autorisé de manière officielle par le SPC ou par le ministère ou organisme) contenues dans le SGI (p. ex. pour respecter une ordonnance de communication d'un État étranger).

L'entrepreneur doit s'assurer, dans la mesure du possible, que tout le trafic sur le réseau national (c.-à-d. le trafic partant d'une partie du Canada vers une destination ou une personne située dans une autre partie du Canada) s'effectue exclusivement au Canada, conformément à l'Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI) du SCT.
https://www.canada.ca/fr/secretariat-conseil-tresor/services/technologie-information/avis-mise-oeuvre-politique/orientation-relative-residence-donnees-electroniques.html

Voici des exemples de la façon dont les exigences en matière de souveraineté des données seraient appliquées aux divers éléments de données recueillis et stockés par les entrepreneurs.

Exemples de champ de données	Doit demeurer au Canada?	Protégé?
***Adresse IP**	Oui	Oui
***Adresse MAC**	Oui	Oui
***Plan d'étage avec appareils indiqués**	Oui	Oui
***Emplacement des appareils – adresse/édifice, étage, salle**	Oui	Oui
Nom du ministère ou de l'organisme	Non	Non
Emplacement des appareils – ville, province, code postal	Non	Non
Adresse de facturation – rue, ville, province, code postal, étage	Non	Non
Fonctions de l'appareil (copie, impression, numérisation, télécopieur)	Non	Non
Personne-ressource opérationnelle (nom, téléphone, courriel)	Non	Non
Numéro d'inventaire du client	Non	Non
Numéro de série	Non	Non
Fabricant	Non	Non
Nom du modèle	Non	Non
Numéro d'inventaire du client	Non	Non
En réseau	Non	Non
Lecture de compteur/nombre d'impressions	Non	Non
Numéro de télécopieur	Non	Non
Nom de la file d'attente d'impression	Doit être évalué au cas par cas	Doit être évalué au cas par cas
Instructions spéciales	Doit être évalué au cas par cas	Doit être évalué au cas par cas
Commentaires	Doit être évalué au cas par cas	Doit être évalué au cas par cas

*Les quatre premiers éléments de données (adresse IP, adresse MAC, plan d'étage avec appareils indiqués et emplacement des appareils) sont considérés par le GC comme étant des renseignements de nature délicate. Sur une base individuelle, certains éléments d'information correspondent à la définition de données de niveau Protégé A, tandis que d'autres correspondent à la définition de données de

niveau Protégé B. Le regroupement potentiel de ces données dans un système en fait des données de niveau Protégé B.

Tout autre élément d'information non énuméré ci-dessus doit être évalué au cas par cas afin de s'assurer qu'il est conforme aux exigences de souveraineté des données du GC, aux autres exigences de sécurité du GC et aux lois sur la protection des renseignements personnels.

Il est recommandé de conserver au Canada les renseignements qui ne sont pas requis pour une facture particulière ou pour la gestion de base des services et de la flotte.

Un exemple de moyen pour répondre à l'exigence de souveraineté des données du GC est que l'entrepreneur peut appliquer des variables nulles comme « emplacement n^{o} 1 » et les lier à l'emplacement de l'appareil dans l'édifice gouvernemental de SPC, rue XXX, à Ottawa. Dans ce cas, « l'emplacement n^{o} 1 » peut être transféré tandis que les détails de l'emplacement de l'appareil demeurent au Canada.

27 IDENTIFICATION ET AUTHENTIFICATION DE L'APPAREIL *(SGI)*

Le SGI doit permettre de s'assurer que les appareils (y compris les appareils portables) sont identifiés et autorisés avant d'être connectés au réseau.

28 ÉLIMINATION OU RETRAIT DE L'INFRASTRUCTURE ET DES APPAREILS *(AMF ET SGI)*

L'élimination ou le retrait de l'infrastructure, des appareils d'impression, des AMF ou des autres appareils des services d'impression d'ATMT des emplacements du GC doit se faire en conformité avec les directives en conseils en matière de sécurité du CST sur l'effacement et la déclassification des supports d'information électroniques (https://www.cse-cst.gc.ca/fr/node/270/html/10572).

Avant l'élimination ou le retrait de l'infrastructure, des appareils d'impression, des AMF ou des autres appareils des services d'impression d'ATMT des emplacements du GC, l'entrepreneur doit assurer le suivi, le contrôle et la vérification du nettoyage des supports, comme suit :

a. tester l'équipement et la procédure de nettoyage pour vérifier leur bon fonctionnement;
b. mener les activités de nettoyage des supports conformément aux exigences du document ITSG-06 (https://www.cse-cst.gc.ca/en/node/270/html/10572);
c. consigner les activités de nettoyage des supports;
d. demander l'approbation de SPC ou du ministère ou de l'organisme avant l'élimination ou le retrait du matériel d'un emplacement du GC.

29 PROTECTION DES DOCUMENTS LORS DE L'IMPRESSION, DE LA COPIE ET DE LA NUMÉRISATION *(AMF)*

L'AMF doit être en mesure de protéger le document de l'utilisateur contre toute divulgation ou modification non autorisée.

30 CAPACITÉ DE CHIFFREMENT *(AMF)*

L'AMF doit être doté d'une capacité de chiffrement pour chiffrer les données des images de documents stockées temporairement (pour réduire la « fenêtre » en cas d'attaque du réseau) et pour protéger les données en cas de défaillance des processus normaux de réécriture de l'AMF due à une panne de courant ou un bourrage papier.

31 EFFACER LES DOCUMENTS NON RÉCLAMÉS *(AMF ET SGI)*

Le SGI et les appareils multifonctions (AMF) doivent avoir la capacité d'effacer les documents non réclamés après un délai préétabli ou prédéterminé par SPC ou par le ministère ou l'organisme.

32 TRAITEMENT DES ERREURS *(SGI)*

Le SGI doit :

a. détecter les erreurs pouvant avoir une incidence sur la sécurité (p. ex. événements de sécurité);
b. générer des messages d'erreur qui fournissent les renseignements nécessaires aux administrateurs pour prendre des mesures correctives sans révéler, dans les relevés d'erreurs et les messages administratifs, des renseignements de nature délicate et potentiellement dangereux qui pourraient être exploités par des adversaires;
c. ne communiquer les messages d'erreur qu'au personnel autorisé, sans révéler des renseignements de nature délicate qui pourraient être utilisés pour inférer ou extrapoler une vulnérabilité dans le système.

33 ATTESTATION POUR LE SITE DE L'INSTALLATION *(SGI)*

L'entrepreneur doit détenir ou obtenir de la Direction de la sécurité industrielle canadienne (DSIC) de TPSGC une attestation de sécurité d'installation (ASI) avec autorisation de détenir des renseignements (ADR) pour le SGI et les installations du portail de prestation de services qui sont à l'extérieur des locaux du GC, au niveau précisé dans la Liste de vérification des exigences relatives à la sécurité (LVERS).

L'entrepreneur qui gère ou soutient le SGI doit obtenir une vérification d'organisation désignée (VOD) auprès de la DSIC.

De plus, les ministères peuvent exiger un filtrage de sécurité supplémentaire pour avoir accès (physiquement ou logiquement) aux SGI.

34 DÉFAILLANCE DANS UN ÉTAT CONNU *(AMF ET SGI)*

Le SGI et les appareils d'impression doivent conserver leur état de configuration (mots de passe, paramètres de service, etc.) après une mise hors tension ou un redémarrage.

35 DISPOSITIFS DE STOCKAGE NON VOLATILS REMPLAÇABLES CHEZ L'UTILISATEUR *(AMF)*

L'AMF doit pouvoir protéger l'information confidentielle du système ou les documents qui peuvent se trouver dans les dispositifs de stockage non volatils remplaçables chez l'utilisateur contre toute exposition si un tel dispositif est retiré de l'AMF, y compris par l'utilisation du chiffrement des données, à moins que d'autres mécanismes de protection approuvés par le GC ne soient utilisés.

36 PROTECTION DES DONNÉES DU GC *(SGI)*

L'entrepreneur s'occupant du SGI doit gérer la sécurité de l'information des ministères et des organismes à toutes les étapes du cycle de vie des renseignements ou du service d'impression afin de veiller à ce que les exigences liées à la sécurité soient établies et à ce que les risques soient mitigés dès le début, que les mesures de contrôle de sécurité soient examinées, que la direction donne son autorisation avant le début de l'opération et que l'autorisation soit maintenue par un contrôle continu du bilan en matière de sécurité.

37 IDENTIFICATION ET AUTHENTIFICATION (UTILISATEURS ORGANISATIONNELS) *(AMF ET SGI)*

Le SGI et le portail de prestation de services doivent identifier et authentifier de façon unique les opérateurs (ou les processus agissant au nom des opérateurs), les administrateurs et les utilisateurs.

Le SGI et l'appareil d'impression doivent être capables d'effectuer l'identification et l'authentification localement ou grâce à un serveur externe (comme Active Directory, LDAP ou Kerberos).

L'authentification de l'utilisateur doit être conforme au Guide sur l'authentification des utilisateurs du CST (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf).

Si l'un des ministères ou organismes l'exige, les appareils d'impression devront satisfaire aux exigences suivantes :

a. les utilisateurs doivent s'authentifier sur l'appareil pour lancer une tâche d'impression, de numérisation ou de photocopie;
b. les appareils d'impression sont en mesure d'authentifier les utilisateurs lorsque ces derniers présentent un badge RFID (en fonction du site et de l'appareil);
c. les appareils d'impression sont en mesure d'authentifier les utilisateurs auprès de l'appareil d'une autre manière qu'avec un badge RFID;
d. les utilisateurs s'authentifient en utilisant le service d'annuaire d'entreprise (généralement Active Directory). Seuls les utilisateurs disposant d'un compte de répertoire réseau actif pourront utiliser l'appareil. Les comptes locaux sur l'appareil ne doivent être autorisés que dans des cas exceptionnels;
e. les appareils d'impression prennent en charge les connexions au serveur LDAPv3 (ou plus récent) pour l'authentification Active Directory.

Si le ministère ou l'organisme l'exige, le SGI des locaux du GC doit avoir une capacité d'authentification par carte à puce, y compris par l'installation de lecteurs de carte à puce (intégré ou par câble USB) et de pilotes de lecteur de carte à puce. Si l'authentification par carte à puce est activée, les ports USB doivent être accessibles pour accepter l'insertion de jetons de carte à puce USB.

Le SGI des locaux du gouvernement du Canada doit utiliser les mécanismes d'authentification résistants aux attaques par réinsertion déterminés par SPC ou par le ministère ou l'organisme pour l'accès réseau aux comptes privilégiés. ***(SGI)***

38 TRAITEMENT DES INCIDENTS *(SGI)*

L'entrepreneur doit démontrer qu'il peut mettre en place une capacité de traitement des incidents en cas d'incident de sécurité relatif aux SGI ou aux PPS. Cette capacité touche entre autres la préparation, la détection et l'analyse, le confinement, l'éradication et la récupération. Les preuves d'une telle capacité pourraient inclure :

a. la coordination des activités de traitement des incidents avec les activités de planification d'urgence;

b. des procédures relatives à :
   i) l'intégration des leçons tirées des activités de traitement des incidents en cours à des mesures de réponse aux incidents, ainsi qu'à des formations, essais et exercices;
   ii) la mise en œuvre des changements qui s'imposent à la lumière de ces leçons.

En cas d'incident de sécurité, SPC ou le ministère ou organisme peut demander à l'entrepreneur de créer une demande de changement d'urgence :

   i) dans les délais précisés par SPC ou par le ministère ou l'organisme, et pour chaque mesure d'atténuation exigée par SPC ou par le ministère ou l'organisme pour maîtriser un incident de sécurité;
   ii) en fonction de la gravité, comme précisé par SPC ou par le ministère ou l'organisme, et pour chaque mesure d'atténuation exigée par SPC ou par le ministère ou l'organisme pour maîtriser un incident de sécurité.
   iii) Il devra également mettre en œuvre la demande de changement d'urgence conformément au niveau de priorité établi par SPC ou par le ministère ou l'organisme.

L'entrepreneur doit définir les mesures à prendre en cas d'incident pour assurer la continuité du service en fonction de la gravité et de la catégorie de l'incident.

a. L'entrepreneur doit amorcer des procédures d'intervention en cas d'incident de sécurité en fonction de sa gravité, comme précisé par SPC ou par le ministère ou l'organisme.
b. L'entrepreneur doit signaler toutes les atteintes présumées ou réelles à la protection des renseignements personnels et de la sécurité relatives aux SGI par téléphone ou par courriel (à une fréquence convenue) à SPC ou aux ministères et organismes, conformément aux lignes directrices du Plan de gestion des événements de cybersécurité du gouvernement du Canada (https://www.canada.ca/fr/secretariat-conseil-tresor/services/acces-information-protection-reseignements-personnels/gestion-securite-identite/plan-gestion-evenements-cybersecurite-gouvernement-canada.html).

L'entrepreneur doit mettre en œuvre une capacité d'intervention en cas d'incidents de fuite d'information, y compris :

a. déterminer quels sont les renseignements qui ont été touchés par la contamination du système d'information;
b. intervenir en cas de fuite d'information en alertant les employés appropriés du GC, en isolant les composantes contaminées du SGI, en éliminant l'information des composantes contaminées et en déterminant quels autres systèmes d'information ou composantes du SGI pourraient avoir été contaminés par la suite;
c. offrir une formation sur l'intervention en cas de fuite d'information aux administrateurs désignés.

39 SURVEILLANCE DES INCIDENTS *(SGI)*

Le SGI doit mettre en œuvre une surveillance procédurale et administrative des incidents afin de détecter les attaques et les utilisations non autorisées du SGI. Cela comprend des mécanismes (p. ex. activités procédurales et administratives) approuvés par SPC pour aider au suivi et à la documentation des incidents de sécurité ainsi qu'à la collecte et à l'analyse de l'information.

40 SIGNALEMENT DES INCIDENTS *(SGI)*

L'entrepreneur doit fournir des mécanismes de signalement et d'atténuation des incidents de sécurité, y compris, mais sans s'y limiter :

a. générer des avertissements ou des rapports sur l'activité du système en fonction des paramètres de sécurité;
b. mettre fin à l'accès ou générer un rapport lorsque des atteintes potentielles à la sécurité sont détectées;
c. préserver et communiquer les données de vérifications indiquées lorsque des atteintes potentielles à la sécurité sont détectées;
d. fournir toutes les preuves relatives à un incident de sécurité à SPC ou aux ministères et organismes.

41 POLITIQUE ET PROCÉDURES D'INTERVENTION EN CAS D'INCIDENT *(SGI)*

L'entrepreneur doit démontrer qu'il dispose d'une politique, d'une procédure et d'un plan officiels et documentés pour faciliter la mise en œuvre et le maintien des activités d'intervention en cas d'incident de sécurité. L'entrepreneur doit se conformer aux procédures de traitement des incidents du Centre des opérations de sécurité (COS) du GC.

42 TRAITEMENT ET CONSERVATION DES SORTIES D'INFORMATION *(SGI)*

Le SGI doit traiter et retenir à la fois les données dans le système d'information et les sorties de données conformément aux lois applicables aux ministères et organismes, aux directives du SCT sur la tenue de documents (http://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=16552) et à la Politique sur la gestion de l'information (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=12742).

43 INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION *(AMF ET SGI)*

Tous les appareils doivent être enregistrés et suivis dans un répertoire des biens désigné. Les coordonnées de l'autorité responsable de l'appareil doivent être consignées dans ce répertoire des biens. Les identificateurs d'appareil doivent être uniques et enregistrés avec les renseignements appropriés sur le propriétaire, la configuration, l'emplacement et l'utilisation. Tous les renseignements doivent être tenus à jour et exacts.

L'entrepreneur doit fournir une liste des composants du SGI installés dans les locaux du gouvernement du Canada, qui comprend tout le matériel et les logiciels et :

a. qui reflète précisément leur configuration courante;
b. qui respecte le niveau de précision jugé nécessaire au suivi et à l'établissement des rapports;
c. qui comprend suffisamment d'informations pour exercer une reddition de comptes efficace à l'égard des biens;
d. qui est accessible à des fins d'examen et de vérification par SPC et par le ministère ou l'organisme;

e. qui est mise à jour au cours des installations et retraits des composants ainsi que des mises à jour du SGI par SPC ou par le ministère ou l'organisme.

44 INVENTAIRE DES COMPOSANTS DU SYSTÈME D'INFORMATION (SGI)

L'entrepreneur doit présenter une configuration du SGI aux fins d'approbation par SPC ou par le ministère ou organisme. L'entrepreneur ne déploiera que les composants et les configurations évalués et approuvés.

L'entrepreneur doit demander l'approbation de SPC ou du ministère ou de l'organisme pour tout écart par rapport aux configurations actuellement déployées dans l'inventaire des composants du SGI.

45 FONCTIONNALITÉ MINIMALE *(AMF ET SGI)*

L'entrepreneur doit s'assurer que les composants et les applications du SGI sont installés et maintenus dans une configuration à sécurité renforcée.

L'entrepreneur doit s'assurer que le SGI et les appareils d'impression n'utilisent que les fonctions autorisées. Il doit également déterminer quelles fonctions sont inutiles ou non sécurisées, comme des ports, des protocoles et des services, et les désactiver (par exemple, désactiver l'accès Internet et les ports USB).

L'entrepreneur doit appliquer une politique de refus global et d'autorisation par exception afin de ne permettre que l'exécution de services logiciels autorisés sur le SGI.

Les appareils d'impression doivent prendre en charge le filtrage IP et le blocage des ports.

Si l'un des ministères ou organismes l'exige, le SGI et les appareils d'impression devront satisfaire aux exigences suivantes :

a. être capable de restreindre l'accès aux ports USB par des moyens logiques ou physiques; empêcher physiquement l'accès à l'USB si le port USB est utilisé à des fins d'authentification;
b. ne pas autoriser les AMF à numériser vers une clé USB ou un protocole SMTP;
c. attribuer des adresses IP statiques aux appareils d'impression.

46 PRIVILÈGE MINIMUM *(SGI)*

Le SGI doit interdire les fonctions ou les accès privilégiés non autorisés par des utilisateurs non privilégiés à l'infrastructure et aux appareils du service d'impression d'ATMT. L'entrepreneur doit mettre en œuvre un contrôle de l'accès fondé sur le rôle (RBAC) avec les stratégies de groupe (GPO) appropriées pour s'assurer que les utilisateurs non autorisés ou non privilégiés ne sont pas en mesure d'accéder à des renseignements privilégiés ou d'exécuter des fonctions privilégiées.

L'entrepreneur doit utiliser le principe du droit d'accès minimal, ce qui autorise l'accès uniquement aux utilisateurs (ou aux processus exécutés en leur nom) qui en ont besoin pour accomplir les tâches qui leur ont été assignées conformément aux missions et aux fonctions opérationnelles de l'organisation.

Le portail de prestation de services doit avoir un mécanisme de contrôle d'accès aux données du SGI qui limite l'accès de l'administrateur ou de l'utilisateur d'un ministère ou organisme aux données de son ministère ou organisme seulement. Par exemple, l'administrateur ou l'utilisateur du ministère_1 ne peut accéder qu'aux renseignements du ministère_1 et ne peut accéder aux renseignements des autres ministères.

47 PERSONNEL DE MAINTENANCE *(AMF ET SGI)*

L'entrepreneur doit démontrer la mise en place d'un processus d'autorisation pour le personnel de maintenance.

L'entrepreneur doit tenir une liste à jour des organisations ou du personnel de maintenance autorisés.

L'entrepreneur doit s'assurer que le personnel chargé de la maintenance pour le service ou les appareils d'impression possède les autorisations d'accès requises.

Si le personnel de maintenance ne possède pas les autorisations d'accès requises, les activités de maintenance doivent être supervisées par le personnel autorisé désigné ayant les autorisations d'accès requises et les compétences techniques jugées nécessaires.

48 OUTILS DE MAINTENANCE

L'utilisation d'outils de maintenance avec le SGI doit être approuvée par SPC ou par le ministère ou l'organisme. Avant de procéder au retrait, tout outil de maintenance ou support connexe doit être vérifié par SPC ou par le ministère ou l'organisme. Tout outil ou support contenant des renseignements du GC doit être nettoyé, détruit ou explicitement autorisé à être retiré par le GC.

49 ACCÈS AUX SUPPORTS *(SGI)*

L'entrepreneur doit limiter l'accès aux supports de TI (numériques et non numériques) contenant des données du SGI aux administrateurs autorisés.

L'entrepreneur doit contrôler et conserver en toute sécurité les données de nature délicate se trouvant sur tout support informatique (numérique et non numérique).

Le SGI doit contrôler et protéger les supports du système d'information pendant le transport en ayant recours à un gardien désigné, conformément à la ligne directrice G1-009 de la GRC, Transport et transmission de renseignements protégés ou classifiés.

50 NETTOYAGE DES SUPPORTS *(SGI)*

L'entrepreneur doit effectuer un nettoyage des supports de systèmes d'information, tant numériques que non numériques, avant leur élimination ou leur réutilisation, que ces supports soient considérés ou non comme amovibles.

L'entrepreneur ne doit retirer aucun support de système d'information (numérique ou non numérique) avant qu'il ait été nettoyé par l'entrepreneur et approuvé par SPC ou par le ministère ou l'organisme, qu'il puisse être retiré ou non des locaux du ministère ou de l'organisme.

Le nettoyage des supports doit être effectué et documenté conformément aux conseils en matière de sécurité des technologies de l'information ITSG-06 du CST du Canada (https://www.cse-cst.gc.ca/fr/node/270/html/10572; capacité de réécriture équivalent à la norme DoD 5502, minimum de 3x, en utilisant un utilitaire de réécriture approuvé par SPC ou par le ministère ou l'organisme).

51 SURVEILLANCE DE L'ACCÈS PHYSIQUE *(SGI)*

L'entrepreneur doit surveiller l'accès physique au portail de prestation de services du SGI pour s'assurer qu'il n'y ait pas d'accès non autorisé, par les moyens suivants :

a. surveillance en temps réel des alarmes d'intrusion physique et de l'équipement de surveillance;

b. enregistrement de tous les événements d'accès physique;
c. présentant des registres à la demande de SPC ou du ministère ou de l'organisme;
d. créant un incident de sécurité à la découverte d'une activité anormale.

52 SURVEILLANCE DU RÉSEAU *(SGI)*

Le gouvernement du Canada doit avoir la capacité de surveiller et d'analyser le trafic en ce qui concerne les services d'impression d'ATMT. La mise en œuvre exacte de la capacité de surveillance du réseau dépendra de l'architecture proposée* en ce qui concerne les éléments de gestion de l'entrepreneur ainsi que l'utilisation et la maintenance du portail de prestation de services. Il est à noter que cela peut nécessiter l'installation de capteurs, fournis comme équipement fourni par le gouvernement (EFG), pour permettre une capture soutenue de tout le trafic sur le réseau de la couche IP et des interactions entre le Canada et le service d'impression d'ATMT, avec la capacité d'inspecter le trafic chiffré lors des communications vers et depuis Internet ou tout autre point d'interconnexion du réseau. L'entrepreneur ne doit apporter aucune modification aux mesures de surveillance du réseau de l'équipement de SPC situé à chaque point de prestation de services sans avoir l'approbation de SPC. De plus, le Canada se réserve le droit d'installer ou de demander à l'entrepreneur d'installer en son nom, à des fins de surveillance du réseau, des applications logicielles développées par le Canada sur des systèmes informatiques et de communication, y compris, mais sans s'y limiter, des postes de travail, des serveurs, des appareils mobiles et de l'équipement de réseau.

* Remarque : S'il est jugé que l'architecture proposée exige l'installation de capteurs, d'applications logicielles développées par le Canada ou d'autres équipements de surveillance du GC dans les installations de l'entrepreneur, l'entrepreneur aura la possibilité de soumettre une autre architecture pour examen ou devra autrement accepter le déploiement du système de surveillance stipulé par le Canada.

53 MAINTENANCE EXTERNE *(SGI)*

Le SGI doit appuyer les activités de maintenance et de diagnostic externes (c.-à-d. la gestion à distance sur un réseau) pour appuyer la gestion du cycle de vie au sein de l'infrastructure afin de maintenir (c.-à-d. réparation et mise à niveau des composants, mise à jour des fichiers de licence, etc.) les biens installés dans l'environnement sans avoir besoin d'un accès à la console dans les centres de données du GC. Cela comprend :

a. autoriser et surveiller les activités de maintenance et de diagnostic externes;
b. permettre l'utilisation d'outils de maintenance et de diagnostic externes comme approuvé par SPC ou par le ministère ou l'organisme et comme documenté dans le plan de sécurité du SGI, qui doit inclure les politiques et procédures pour l'établissement et l'utilisation de connexions de maintenance et de diagnostic externes;
c. permettre l'utilisation d'authentifiants au niveau d'assurance 3 (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.30.031v2-eng.pdf) pour établir des sessions de maintenance et de diagnostic externes;
d. obtenir l'approbation nécessaire pour chaque session de maintenance externe (à distance) et aviser le personnel approprié;
e. tenir à jour, examiner et vérifier les dossiers relatifs aux activités de maintenance et de diagnostic externes;

f. permettre l'utilisation de mécanismes cryptographiques pour protéger l'intégrité et la confidentialité des communications liées aux activités de maintenance et de diagnostic externes (à distance);

g. restreindre les privilèges des comptes utilisés pour la maintenance externe au minimum requis;

h. s'assurer que les comptes utilisés pour la maintenance externe (à distance) sont désactivés lorsqu'ils ne sont pas utilisés.

54 ENVIRONNEMENTS NON LIÉS À LA PRODUCTION *(SGI)*

L'entrepreneur doit séparer (par des moyens logiques ou physiques) les environnements de production et non liés à la production (comme les environnements de développement et d'essai) et imposer la séparation au moyen de contrôles d'accès pour prévenir les modifications ou les accès non autorisés aux ressources d'information.

Toute connectivité entre les environnements de production et non liés à la production doit être autorisée et doit être documentée avec exactitude et exhaustivité afin d'établir les fonctions requises et les contrôles de sécurité attribués pour maintenir le niveau de protection correspondant à la sensibilité de l'information.

L'entrepreneur ne doit pas utiliser les données de production à des fins d'essai ou de développement.

55 AUTHENTIFICATION PAR MOT DE PASSE *(SGI)*

Lorsque l'authentification PAR MOT DE PASSE pour les utilisateurs finaux est utilisée pour l'accès au portail de prestation de services et aux SGI :

a. le système d'information, pour l'authentification par mot de passe, exige un degré de complexité minimal du mot de passe fondé sur des exigences approuvées par le gouvernement du Canada relatives à sensibilité à la casse, au nombre de caractères, à la combinaison de lettres majuscules, de lettres minuscules, de chiffres et de caractères spéciaux, y compris les exigences minimales pour chaque type (par exemple, au moins huit caractères, au moins trois des groupes suivants : majuscules, minuscules, nombres et caractère spécial);

b. pour l'authentification fondée sur le mot de passe, le système d'information exige la modification d'un nombre prédéfini de caractères lors du changement de mot de passe;

c. pour l'authentification fondée sur le mot de passe, le système d'information ne stocke et ne transmet que les mots de passe protégés par une cryptographie approuvée par le CST; (ITSP.40.111, voir la page https://www.cse-cst.gc.ca/en/publication/list/Cryptography);

d. pour l'authentification fondée sur le mot de passe, le système d'information applique des restrictions quant à la durée de vie minimale et maximale des mots de passe, en respectant les valeurs approuvées par le gouvernement du Canada pour la durée de vie minimale (au moins 1 jour) et maximum (par exemple, 90 jours);

e. pour l'authentification fondée sur le mot de passe, le système d'information interdit la réutilisation des mots de passe pendant un nombre de générations déterminé par le GC;

f. pour l'authentification fondée sur le mot de passe, le système d'information permet l'utilisation d'un mot de passe temporaire servant à l'ouverture d'une session pourvu que celui-ci soit changé immédiatement pour un mot de passe permanent après cette ouverture.

Toute exception aux exigences d'authentification par mot de passe doit être approuvée par SPC ou par le ministère ou l'organisme.

56 ACTIVITÉS PERMISES SANS IDENTIFICATION NI AUTHENTIFICATION *(AMF ET SGI)*

Le SGI doit empêcher l'accès aux composants ou aux ressources de l'infrastructure sans identification, authentification et autorisation.

57 VÉRIFICATION DE SÉCURITÉ DU PERSONNEL *(AMF ET SGI)*

L'entrepreneur doit s'assurer que tout le personnel se conforme aux exigences en matière d'habilitation de sécurité du personnel précisées dans la Liste de vérification des exigences relatives à la sécurité (LVERS).

58 CESSATION D'EMPLOI DU PERSONNEL *(AMF ET SGI)*

L'entrepreneur doit, lors de la cessation d'emploi d'un employé dont les tâches étaient liées aux SGI :

a. mettre fin à tout accès aux SGI pour l'employé, y compris l'accès à distance;
b. récupérer tous les biens liés à la sécurité (p. ex. carte d'identité de l'employé, jeton d'authentification physique);
c. aviser la Direction de la sécurité industrielle canadienne (DSIC) pour qu'elle mette fin aux désignations de filtrage du personnel.

59 CONTRÔLE D'ACCÈS PHYSIQUE DU PERSONNEL *(AMF ET SGI)*

L'entrepreneur doit mettre en œuvre des contrôles d'accès physique fondés sur les rôles pour le SGI qui comprennent ce qui suit :

a. tenir à jour une liste du personnel autorisé à accéder aux installations;
b. assurer la séparation des tâches lorsque l'autorisation d'accéder aux installations est accordée par une autre personne que celle qui autorise l'accès aux SGI;
c. donner accès aux installations au personnel autorisé possédant un justificatif d'identité approuvé.

60 AUTHENTIFICATION FONDÉE SUR L'ICP *(AMF ET SGI)*

Dans l'éventualité où une authentification fondée sur l'ICP pour les utilisateurs finaux est requise pour accéder au portail de prestation de services, aux SGI ou aux AMF, les exigences suivantes doivent être respectées :

a. pour l'authentification fondée sur l'ICP, le système d'information valide les certificats en créant un chemin de certification avec l'information d'état vers un point d'ancrage de confiance autorisé. Il vérifie aussi l'information d'état des certificats;
b. pour l'authentification fondée sur l'ICP, le système d'information applique une politique d'accès autorisé à la clé privée correspondante;
c. pour l'authentification fondée sur l'ICP, le système d'information associe l'identité authentifiée au compte d'une personne ou d'un groupe;
d. pour l'authentification fondée sur l'ICP, le système d'information utilise une mémoire cache locale de données de révocation afin de prendre en charge la découverte et la validation de chemins au cas où il devenait impossible d'accéder à l'information de révocation au moyen du réseau.

Toute exception doit être explicitement approuvée par SPC ou par le ministère ou l'organisme.

61 NOTIFICATION D'OUVERTURE DE SESSION PRÉCÉDENTE (ACCÈS) *(SGI)*

À l'ouverture de session (accès), le SGI doit informer les administrateurs et les opérateurs de la date et de l'heure de la dernière ouverture de session (accès), lorsque cela est techniquement possible et disponible en option, en utilisant des produits existants qui ne nécessitent pas de solutions supplémentaires ou personnalisées.

62 PROTECTION DE L'INFORMATION DE VÉRIFICATION *(AMF ET SGI)*

Le SGI et les AMF doivent :

a. protéger l'information relative à la vérification contre les accès, les modifications ou les suppressions non autorisés;
b. utiliser des mécanismes de chiffrement inviolables pour protéger la confidentialité de l'information relative à la vérification au besoin;
c. sauvegarder les dossiers de vérification dans un autre système ou format que celui qui fait l'objet d'une vérification, selon un calendrier précisé par SPC ou par le ministère ou organisme.

Les registres doivent être archivés pendant une période de temps suffisante pour appuyer les vérifications de conformité aux règlements et aux politiques. Pour ce faire, il faut :

a. sauvegarder les journaux pendant au moins six mois;
b. conserver les événements et les journaux associés à un incident de sécurité dans le SGI pendant au moins deux ans.

63 PROTECTION DE L'INFORMATION INACTIVE *(AMF ET SGI)*

Le SGI et les appareils multifonctions doivent protéger la confidentialité et l'intégrité des données stockées du gouvernement du Canada, y compris par l'utilisation de solutions cryptographiques avec cryptographie approuvée par le CST (ITSP.40.111) et de technologies et processus de gestion des clés, à moins que d'autres mécanismes de protection approuvés par le GC ne soient utilisés. L'intégrité des données du GC doit être maintenue afin d'empêcher et de détecter toute modification, copie ou destruction inappropriée (double saisie, authentification de message, signature numérique, totaux de contrôle, etc.).

64 SÉPARATION RÉSEAU-TÉLÉCOPIEUR DU RTPC *(AMF)*

Tout AMF doté d'une fonction de télécopieur doit être conforme aux exigences en matière de télécopie définies dans le profil de protection « Protection Profile for Hardcopy Devices » (version 1.0, 10 septembre 2015, IPA, NIAP et la communauté technique des AMF). La séparation entre le réseau et le télécopieur du réseau téléphonique public commuté (RTPC) doit garantir que le modem télécopieur du RTPC ne puisse pas être utilisé pour créer un pont entre les données du RTPC et du réseau local. L'AMF interdit toute communication par l'interface du télécopieur, à l'exception de la transmission ou de la réception de données utilisateur à l'aide des protocoles du télécopieur. Les cas de test inclus dans les annexes du profil de protection doivent être utilisés pour les tests et évaluations de la sécurité au cours du processus d'évaluation de la sécurité et d'autorisation. Si un ministère ou organisme l'exige, la fonction de télécopieur ne doit pas être intégrée à l'appareil avant que SPC ou le ministère ou l'organisme n'ait donné son approbation.

65 CONTENU ACCESSIBLE AU PUBLIC *(SGI)*

L'entrepreneur doit obtenir l'approbation de SPC avant de rendre accessible au public le contenu du SGI.

66 ACCÈS À DISTANCE *(SGI)*

La gestion à distance du SGI doit être effectuée à l'aide d'une méthode approuvée par SPC qui comporte ce qui suit :

a. la gestion à distance doit être limitée aux emplacements du SGI approuvés par le gouvernement du Canada, avec des consoles de gestion dédiées;
b. la 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. la détection des cas de gestion à distance non autorisée;
d. l'autorisation de la gestion à distance avant de permettre la connexion;
e. l'utilisation de mécanismes automatisés pour faciliter la surveillance et le contrôle des méthodes de gestion à distance;
f. l'acheminement de tous les dossiers de télégestion aux SGI à l'aide d'un nombre limité de points de contrôle d'accès gérés;
g. la protection de l'information sur les mécanismes de gestion à distance contre l'utilisation et la divulgation non autorisées;
h. la mise en œuvre de mécanismes cryptographiques pour protéger la confidentialité et l'intégrité de l'information lors des sessions d'accès à distance;
i. toute connexion servant à la gestion à distance doit être consignée et le GC doit avoir une visibilité sur le trafic non crypté.

L'entrepreneur doit autoriser l'exécution de commandes privilégiées et l'accès à l'information relative à la sécurité au moyen d'un accès à distance pour la gestion du SGI, comme approuvé par SPC ou par le ministère ou l'organisme.

Si l'accès à distance est fourni par l'entrepreneur, ce dernier doit satisfaire aux exigences suivantes, conformément à l'approbation de SPC ou du ministère ou de l'organisme :

a. authentification à deux facteurs;
b. journalisation détaillée des accès et du système alimentant le système de gestion de l'information et des événements de sécurité de l'entrepreneur ou du GC, comme déterminé par SPC ou par le ministère ou l'organisme;
c. vérification exhaustive des sessions pour tous les accès privilégiés et stockage des enregistrements pendant 90 jours civils;
d. terminal dédié à sécurité renforcée (poste de travail ou ordinateur portable), comme approuvé par SPC ou par le ministère ou l'organisme;
e. méthodes autorisées et documentées de gestion à distance, directives de mise en œuvre et restrictions d'utilisation;
f. surveillance des accès non autorisés;
g. une connexion de session sécurisée utilisant un niveau de chiffrement accepté selon les normes du CST, comme SSL, TLS 1.2 ou VPN;
h. la conception des solutions d'accès à distance doit être conforme aux exigences de zonage de réseau approuvées par le CST (ITSG-22 et ITSG-38).

67 CONFIGURATION SÉCURISÉE *(AMF)*

L'AMF doit être en mesure de protéger ses paramètres de sécurité contre toute divulgation et modification non autorisées lorsqu'ils sont conservés dans l'AMF et en transfert vers ou depuis une entité informatique externe. L'AMF doit également pouvoir protéger les commutateurs DIP intégrés qui permettent aux utilisateurs de réinitialiser ou désactiver certaines des fonctions de sécurité comme le chiffrement, l'effacement des travaux après une impression réussie, etc.

68 ALERTES, AVIS ET DIRECTIVES DE SÉCURITÉ *(SGI)*

L'entrepreneur doit, de façon continue, surveiller et diffuser les alertes, les avis et les directives en matière de sécurité provenant des organismes externes désignés (p. ex. SPC, le Centre canadien de réponse aux incidents cybernétiques) et y répondre; il doit également mettre en œuvre les directives de sécurité conformément aux échéanciers établis et informer le GC du degré de non-conformité.

69 SENSIBILISATION À LA SÉCURITÉ *(SGI)*

L'entrepreneur doit démontrer la tenue de séances de formation et de sensibilisation en matière de sécurité à l'intention du personnel travaillant avec le SGI, comme suit :

a. dans le cadre de la formation initiale des nouveaux employés;
b. avant d'autoriser l'accès aux SGI ou avant l'exécution des tâches assignées;
c. chaque année, lorsque des changements aux services d'impression ont une incidence sur la sécurité;
d. une formation fondée sur les rôles et les responsabilités du personnel;
e. l'organisation doit conserver les dossiers individuels de formation du personnel pour une période de temps déterminée par SPC ou par le ministère ou l'organisme.

70 INCIDENT DE SÉCURITÉ *(SGI)*

En cas d'incident de sécurité ou à la demande de SPC ou du ministère ou de l'organisme, l'entrepreneur doit participer à toute vérification ou inspection de sécurité demandée par SPC ou par le ministère ou l'organisme en fournissant les renseignements demandés en temps opportun, en fonction de la gravité, comme précisé par SPC ou par le ministère ou l'organisme.

L'entrepreneur doit fournir un rapport sommaire annuel sur la sécurité à SPC ou au ministère ou à l'organisme, y compris des rapports sur le nombre, la gravité et les mesures d'atténuation des incidents liés à la sécurité.

71 EXAMEN DE SÉCURITÉ *(SGI)*

a. Chaque année, l'entrepreneur doit effectuer un examen de conformité pour s'assurer que les exigences en matière de sécurité sont respectées.
b. L'entrepreneur doit fournir les résultats de son examen de conformité sous la forme d'un rapport accompagné de données probantes à des fins d'examen par SPC ou par le ministère ou l'organisme, dans les délais convenus entre l'entrepreneur et SPC ou le ministère ou organisme.
c. Si SPC ou le ministère ou l'organisme juge que les preuves ne démontrent pas la conformité au contrat, l'entrepreneur doit fournir un plan qui corrige les lacunes décelées par SPC ou par le ministère ou l'organisme.

72 ENVOI ET RÉCEPTION DE TÉLÉCOPIES SUR RTPC *(AMF)*

Lors de l'envoi et de la réception de télécopies sur le RTPC, l'AMF doit être en mesure de protéger le document de l'utilisateur contre toute divulgation ou modification non autorisée pendant le transfert du document et lors de son stockage dans l'AMF.

73 SÉPARATION DES TÂCHES *(SGI)*

L'entrepreneur doit :

a. séparer les tâches des personnes par une répartition des rôles et des responsabilités afin de réduire la possibilité qu'une personne compromette un processus critique et de s'assurer que les membres du personnel n'exécutent que les tâches autorisées qui sont pertinentes à leurs fonctions et postes respectifs;
b. consigner la séparation des tâches des personnes;
c. définir les autorisations d'accès au système d'information pour appuyer la séparation des tâches.

74 AUTHENTICITÉ DES SESSIONS *(AMF ET SGI)*

Le SGI doit établir et maintenir l'authenticité de chaque session de communication en ne reconnaissant que les identificateurs de session uniques générés par le système et en invalidant les identificateurs de session lors de la déconnexion ou de toute autre forme de fin de session.

75 VERROUILLAGE DE SESSION *(AMF ET SGI)*

Le SGI doit empêcher tout accès ultérieur au système en déclenchant un verrouillage de session pour l'appareil après une période de temps approuvée par SPC ou par le ministère ou l'organisme, en cas d'inactivité ou à la réception de la demande d'un utilisateur. Les verrouillages de session sont des mesures temporaires prises lorsque les utilisateurs arrêtent de travailler et s'éloignent de la proximité immédiate des systèmes d'information, mais ne veulent pas fermer leur session en raison de la nature temporaire de leur absence. Cela s'effectue généralement au niveau du système d'exploitation, mais peut aussi se faire au niveau de l'application.

Le système d'information doit garder la session verrouillée jusqu'à ce que l'utilisateur rétablisse l'accès en recourant aux procédures d'identification et d'authentification établies.

Verrouillage de session : les appareils informatiques comme les AMF, les serveurs, les postes de travail ou les ordinateurs portables doivent être configurés pour se verrouiller après une période d'inactivité déterminée, et demander à l'utilisateur d'entrer son mot de passe pour déverrouiller l'appareil. Lorsqu'il est activé sur un appareil doté d'un écran, le mécanisme de verrouillage de session du système d'information doit afficher un motif visible au public à l'écran de cet appareil afin de cacher ce qui était auparavant visible à cet écran.

La durée de cette période doit être configurable. S'il n'y a pas de capacité de verrouillage de session sur l'appareil ou si la période de temps définie est une période fixe pour certains systèmes d'exploitation ou applications utilisés par l'AMF ou le SGI, SPC aura besoin d'une analyse de risque plus approfondie afin d'approuver leur utilisation dans le SGI. Toute exception concernant la capacité de verrouillage des sessions des appareils doit être examinée et approuvée par SPC ou par le ministère ou organisme.

76 NETTOYAGE DU STOCKAGE DANS LES DISPOSITIFS FONDÉS SUR LES TRAVAUX *(AMF)*

Les AMF doivent être capables d'effacer de façon sécurisée les données d'impression entre les travaux d'impression. Ceci doit garantir que les données d'impression sont supprimées de façon permanente et ne peuvent être récupérées, peu importe le moyen. Chaque appareil d'impression, y compris les AMF et les autres appareils d'imagerie, doit être configuré de façon à exécuter automatiquement une réécriture à trois passages (3X) ou plus après chaque tâche d'impression. Si une réécriture 3X ne peut être effectuée, l'entrepreneur doit proposer une solution de rechange à SPC ou au ministère ou à l'organisme à des fins d'examen et de considération.

77 CHAÎNE D'APPROVISIONNEMENT ET PROCESSUS D'ACQUISITION *(SGI)*

L'entrepreneur doit se conformer au processus d'évaluation de l'information sur la sécurité de la chaîne d'approvisionnement de SPC pour les produits utilisés dans le SGI. L'entrepreneur ne doit utiliser que des produits qui ont fait l'objet d'une évaluation.

En tout temps pendant la période du contrat, si l'entrepreneur propose d'introduire de nouveaux produits commerciaux sur le réseau du GC, sur l'infrastructure de l'entrepreneur ou sur l'infrastructure d'un tiers et si ces produits sont destinés à être interconnectés avec le réseau du GC, l'entrepreneur doit d'abord obtenir l'approbation écrite du ministère ou de l'organisme et de SPC. Cela comprend tous les nouveaux produits commerciaux qui ne figuraient pas sur la liste des produits de TI approuvée par le ministère ou l'organisme et SPC conformément aux vérifications d'intégrité de la chaîne d'approvisionnement dans la lettre d'approbation de l'équipement – menace pour l'approvisionnement du gouvernement du Canada. SPC et le ministère ou l'organisme se réservent le droit de refuser de nouveaux produits commerciaux, de proposer de nouvelles mesures de protection et de valider et d'approuver de façon indépendante les produits commerciaux si ces produits seront utilisés sur le réseau du GC ou interconnectés avec celui-ci.

En tout temps, si SPC ou le ministère ou l'organisme informe l'entrepreneur qu'un fabricant ou FEO n'est plus considéré comme étant un fabricant ou un FEO de confiance (c.-à-d. qu'il est non fiable), l'entrepreneur doit immédiatement cesser le déploiement de l'équipement fabriqué par ce fabricant ou FEO dans le réseau du GC et dans toute infrastructure de l'entrepreneur qui sera interconnectée avec le réseau du GC. En ce qui concerne l'équipement déjà déployé, l'entrepreneur devra définir ou retirer l'équipement fabriqué par ce fabricant ou FEO du réseau du GC ou de l'infrastructure ou du réseau de base de l'entrepreneur qui sera interconnecté au réseau du GC.

Si l'entrepreneur est informé qu'un tiers déploie un équipement non éprouvé sur son réseau, il doit immédiatement en informer SPC et le ministère ou l'organisme.

78 SERVICES DE TRANSITION À LA FIN DE LA PÉRIODE DU CONTRAT

À la fin du contrat, à la fin de la dernière période d'option ou au moment de la résiliation du contrat, selon le cas, et dans un délai de 40 jours civils après en avoir reçu la demande par écrit de la part du ministère ou de l'organisme ou dans un délai plus long convenu par les parties, l'entrepreneur devra transférer toutes les données et les métadonnées du SGI à SPC ou au ministère ou à l'organisme au moyen d'un mécanisme sécurisé approuvé par ce dernier et dans un format accessible, lisible par machine et utilisable qui soit acceptable pour SPC ou pour le ministère ou l'organisme et sans aucuns frais supplémentaires pour celui-ci. Les données et les métadonnées seront réputées reçues au moment de l'approbation de SPC ou du ministère ou de l'organisme. Cette approbation visera à attester que les données et les métadonnées reçues sont accessibles, lisibles par machines et

utilisables par SPC ou par le ministère ou l'organisme.

À la fin du contrat, à la fin de la dernière période d'option ou au moment de la résiliation du contrat, selon le cas, SPC ou le ministère ou l'organisme peut demander à l'entrepreneur d'enlever le SGI, y compris tout le matériel et les logiciels appartenant à l'entrepreneur et installés dans le SGI, sans frais supplémentaires pour le ministère ou l'organisme, et ce, dans les 40 JOGF suivant la demande de SPC ou du ministère ou de l'organisme. Si l'entrepreneur n'enlève pas le SGI, SPC ou le ministère ou l'organisme peut prendre possession de l'entièreté du SGI.

79 CONFIDENTIALITÉ ET INTÉGRITÉ DES TRANSMISSIONS *(AMF ET SGI)*

Le SGI et les appareils d'impression doivent garantir la confidentialité et l'intégrité de bout en bout des données en transit, y compris par l'utilisation de solutions cryptographiques avec des technologies et des processus de cryptographie et de gestion des clés approuvés par le CST (ITSP.40.111). Cela comprend :

a. la protection des données transmises entre les composants et entre les systèmes autorisés afin de s'assurer que les renseignements sont intacts et qu'ils ne sont pas modifiés pendant le transfert, que ce soit à des fins malveillantes ou par accident;
b. la capacité d'exécuter des vérifications de l'intégrité des fichiers du système source au système cible pour l'échange de données et d'aviser les parties concernées lorsqu'une condition d'erreur est constatée (relativement à une transmission précise ou à des composants du système);
c. l'établissement de voies de communication fiables pour s'assurer que les communications avec les appareils d'impression et le SGI sont effectuées avec des terminaux connus.

80 TENTATIVES INFRUCTUEUSES D'OUVERTURE DE SESSION *(SGI)*

Le SGI, y compris le portail de prestation de services et la console de gestion, doit :

a. appliquer une limite, approuvée par SPC ou par le ministère ou l'organisme, de tentatives consécutives d'ouverture de session non valides par un utilisateur au cours d'une période définie;
b. lorsque le nombre maximal de tentatives infructueuses est dépassé, verrouiller automatiquement le compte et la session pour une période de temps approuvée par SPC ou par le ministère ou l'organisme, verrouiller le compte ou nœud jusqu'à ce qu'il soit déverrouillé par un administrateur, comme indiqué par SPC ou par le ministère ou l'organisme, ou encore, retarder la prochaine invitation à ouvrir une session avec un délai approuvé par SPC ou par le ministère ou l'organisme. Cette mesure de contrôle s'applique peu importe si la tentative d'ouverture de session est effectuée au moyen d'une connexion locale ou de réseau.

81 PISTE DE VÉRIFICATION DE L'UTILISATION ET DE LA CONFIGURATION *(AMF ET SGI)*

Tous les composants du SGI et des AMF doivent consigner les transferts de documents d'impression (y compris les adresses de la source et de destination) ainsi que la date et l'heure du transfert. De plus, tous les composants du SGI et des AMF doivent consigner les accès aux applications résidentes, pour les tentatives d'ouverture de session réussies et non réussies.

82 UTILISATION DE SYSTÈMES D'INFORMATION EXTERNES *(SGI)*

L'entrepreneur doit interdire l'utilisation de systèmes d'information externes pour se connecter physiquement ou logiquement aux SGI et aux appareils d'impression.

83 VÉRIFICATION DES FONCTIONS DES AMF *(AMF)*

L'AMF doit vérifier s'il connaît des défaillances en effectuant un autotest chaque fois qu'il est mis sous tension.

84 VÉRIFICATION DES MISES À JOUR LOGICIELLES *(AMF)*

L'AMF doit garantir que seul le personnel autorisé est autorisé à installer des logiciels, et doit avoir la capacité d'aider l'installateur à vérifier l'authenticité de la mise à jour du logiciel.

85 ÉVALUATION DES VULNÉRABILITÉS *(SGI)*

L'entrepreneur doit démontrer que des évaluations régulières des vulnérabilités sont effectuées aux emplacements où des systèmes du service d'impression d'ATMT sont situés et qui sont en dehors des installations du GC.

À la discrétion et à la demande du GC, l'entrepreneur doit autoriser des tests d'évaluation des vulnérabilités du portail de prestation de services, effectués par le GC ou par un tiers choisi par le GC, sur une base annuelle, dans les 20 JOGF suivant une telle demande. L'entrepreneur doit déterminer l'attribution des responsabilités en ce qui a trait au soutien des tests d'évaluation des vulnérabilités et fournir tout le soutien requis par le GC.

Le GC ou une tierce partie agissant en son nom peut effectuer des tests d'évaluation des vulnérabilités des systèmes de service d'impression d'ATMT situés à l'intérieur ou à l'extérieur des locaux du GC et fournir à l'entrepreneur un rapport d'évaluation des vulnérabilités qui lui indiquera les vulnérabilités détectées. L'entrepreneur doit fournir au GC un rapport sur l'atténuation des vulnérabilités et mettre en œuvre les mesures correctives indiquées dans un délai convenu entre le GC et l'entrepreneur, sans frais pour le GC.

86 ACCÈS SANS FIL *(AMF ET SGI)*

L'entrepreneur doit désactiver toutes les fonctions de réseau sans fil intégrées aux SGI partout où cela tombe sous sa responsabilité. Cela inclut, mais sans s'y limiter, la désactivation des fonctions sans fil dans les serveurs, les outils de gestion des services, les serveurs du portail de prestation de services, les appareils d'impression et les outils du technicien de l'entrepreneur qui sont physiquement ou logiquement connectés au service d'impression d'ATMT.

Dans certaines situations où cela est jugé nécessaire par le ministère ou l'organisme, en s'appuyant sur une évaluation des risques et avec l'approbation de SPC ou du ministère ou de l'organisme, des capacités sans fil peuvent être offertes lorsque toutes les autres options de connectivité pour l'infrastructure du GC ont été épuisées, ou à la demande de SPC ou du ministère ou de l'organisme; les contrôles de sécurité sans fil appropriés doivent être mis en œuvre conformément aux directives du CST (https://www.cse-cst.gc.ca/en/publication/list/Wireless-and-Mobility).

Si un ministère ou organisme l'exige, les AMF peuvent ne devoir avoir aucune capacité sans fil et Bluetooth physique.

87 CAPACITÉS DE ZONAGE *(SGI)*

Le SGI des locaux du gouvernement du Canada doit satisfaire aux exigences énoncées dans les conseils en matière de sécurité des technologies de l'information du CST intitulés Exigences de base en matière de sécurité pour les zones de sécurité de réseau au sein du gouvernement du Canada (ITSG-22) (https://www.cse-cst.gc.ca/fr/system/files/pdf_documents/itsg-22-fra.pdf).

Terme	Définition
Authentification à deux facteurs	L'authentification à deux facteurs est une méthode de confirmation de l'identité affirmée d'un utilisateur où l'accès n'est accordé à un utilisateur qu'après la présentation réussie d'au moins deux éléments de preuve ou facteurs à un mécanisme d'authentification.
Administrateur	Un utilisateur qui est autorisé à effectuer des activités administratives pour les services d'impression des ATMT. L'administrateur du GC est un administrateur qui travaille pour le GC et qui est géré par ce dernier, et l'administrateur de l'entrepreneur ou du fournisseur de services est un administrateur qui travaille pour l'entrepreneur ou le fournisseur de services et qui est géré par ce dernier. Les administrateurs effectuent généralement des activités de configuration, de maintenance et de gestion du service et ont généralement besoin de droits d'accès privilégiés au système.
Contrôle de l'accès	Procédés d'octroi ou de refus des demandes particulières en vue d'obtenir et d'utiliser des services de traitement de l'information ou des données et d'entrer dans des installations physiques particulières. Elles garantissent que les personnes ne peuvent utiliser que les ressources auxquelles elles ont droit, uniquement aux fins approuvées, en assurant l'application des politiques de sécurité qui régissent l'accès à l'échelle de l'entreprise.
Authentification	Mécanisme utilisé pour identifier un utilisateur, généralement en lui fournissant un nom d'utilisateur et un mot de passe, ou d'autres justificatifs d'identité. Ce mécanisme permet de déterminer si l'utilisateur est la personne qu'il prétend être.
Autorisation (Évaluation de la sécurité et autorisation)	Processus continu qui consiste à obtenir et à maintenir une décision de gestion officielle, prise par un cadre supérieur, qui autorise à exploiter un système d'information et à accepter explicitement le risque inhérent à son utilisation pour mener un ensemble d'activités opérationnelles en s'appuyant sur l'application d'un ensemble convenu de contrôles de sécurité et sur les résultats d'une évaluation de sécurité continue.
Disponibilité	Le fait d'être accessible et utilisable de manière fiable et en temps opportun. Remarque : Il est implicite dans la définition que l'intégrité des objets auxquels on accède n'a pas été perdue en raison de leur compromission (par exemple, une information corrompue n'est pas considérée comme disponible, car elle n'est pas utilisable).
DSIC	Direction de la sécurité industrielle canadienne
CCRIC	Centre canadien de réponse aux incidents cybernétiques

Terme	Définition
Certificat	Un certificat de clé publique, dans un format conforme à la recommandation X.509 V3 du Secteur de normalisation des télécommunications de l'Union internationale des télécommunications (ITU-T), comme décrit dans le document rfc5280 (http://www.ietf.org/rfc/rfc5280.txt, en anglais), qui contient la clé publique d'un abonné, qui peut être une personne ou un appareil, avec des renseignements connexes, signé numériquement avec la clé privée de l'autorité de certification qui a émis le certificat.
Gestion du changement	Méthodes et procédures normalisées employées pour traiter efficacement et avec exactitude tous les changements apportés aux services d'impression liés aux ATMT afin de réduire le nombre d'incidents liés à un service et leur incidence.
Critères communs	Abréviation de Critères communs pour l'évaluation de la sécurité des technologies de l'information, des normes internationales pour la certification des mécanismes de sécurité informatique. Les Critères communs sont un cadre dans lequel les utilisateurs de systèmes informatiques peuvent préciser leurs exigences fonctionnelles et d'assurance en matière de sécurité au moyen de profils de protection; les fournisseurs peuvent ensuite mettre en œuvre ou faire des assertions concernant les attributs de sécurité de leurs produits et les laboratoires d'essai peuvent évaluer les produits pour déterminer s'ils répondent réellement à ces assertions.
Compromission	Accès non autorisé aux biens de TI, leur divulgation, leur destruction, leur suppression, leur modification, leur utilisation ou leur interruption, causant une perte de confidentialité, d'intégrité et/ou de disponibilité.
Compromettre	L'acte de provoquer une compromission en exploitant des vulnérabilités. Remarque : Une compromission peut mener à l'échec d'une activité opérationnelle et de ses exigences connexes. Cela peut entraîner des préjudices aux intérêts nationaux ou non nationaux.
Confidentialité	État d'un élément qui peut être divulgué seulement à des individus autorisés. Qualité conférée à des renseignements pour signifier qu'ils ne peuvent être divulgués qu'à des personnes autorisées.
Gestion de la configuration	Méthodes et procédures normalisées pour établir et maintenir les éléments de configuration matériels et logiciels des services d'impression liés aux ATMT.
Justificatif d'identité	Un objet ou des données qui lient de façon définitive une personne à un jeton qui appartient et est contrôlé par cette personne, et qui sont utilisées pour authentifier ou confirmer l'identité d'un individu.
CST	Centre de la sécurité des télécommunications
Criticité	L'importance relative d'une activité opérationnelle en ce qui a trait à la promotion ou au maintien de la santé, de la sûreté, de la sécurité ou du bien-être économique des Canadiens, ou au fonctionnement efficace du gouvernement du Canada.
Ministère ou organisme	Ministère ou organisme

Terme	Définition
Données	Représentation électronique d'information. Quantités, caractères ou symboles sur lesquels un ordinateur effectue des opérations et qui sont enregistrés et transmis sous forme de signaux électriques et enregistrés sur des supports magnétiques, optiques ou mécaniques.
Centre de données	Installation utilisée pour héberger des systèmes informatiques et des composantes connexes, comme des systèmes de télécommunication et de stockage.
Appareil	Un objet physique (p. ex. projecteur, tableau blanc, ordinateur de bureau ou portatif, imprimante, numériseur).
Média numérique	Tout média encodé dans un format lisible par machine. Les médias numériques peuvent être créés, visualisés, distribués, modifiés et préservés sur des appareils électroniques numériques.
Document	Un support et l'information qui y est enregistrée, qui ont généralement une permanence et qui peuvent être lus par une personne ou une machine.
VOD – Vérification d'organisation désignée	Une vérification d'organisation désignée (VOD) permet aux organisations d'obtenir une enquête de sécurité pour leurs employés sur le plan de la cote de fiabilité.
Chiffrement	Le chiffrement consiste à traduire des données dans un code secret. Le chiffrement est la façon la plus efficace de sécuriser des données. Pour lire un fichier chiffré, vous devez avoir accès à une clé secrète ou à un mot de passe qui vous permet de déchiffrer le fichier. Les données non chiffrées sont appelées texte en clair alors que les données chiffrées sont appelées texte chiffré. Source : http://www.webopedia.com/TERM/E/encryption.html (en anglais seulement).
Systèmes d'information externes	Systèmes d'information ou composants de systèmes d'information en dehors des limites d'autorisation des services d'impression liés aux ATMT. Cela peut inclure, par exemple : (i) les systèmes ou appareils d'information personnels (p. ex. ordinateurs portatifs, téléphones intelligents, tablettes, assistants numériques personnels); (ii) les appareils informatiques et de communication privés situés dans des installations commerciales ou publiques (p. ex. hôtels, gares, centres de congrès, centres commerciaux ou aéroports); (iii) les systèmes informatiques qui appartiennent ou sont contrôlés par des organisations non gouvernementales qui ne sont pas dédiées ou autorisées à interagir avec les services d'impression d'ATMT du réseau du gouvernement.
Utilisateur final	Une personne autorisée à utiliser les services d'impression liés aux ATMT.
Dispositif de stockage non volatil remplaçable chez l'utilisateur	Toute unité remplaçable chez l'utilisateur dont le but premier est de fournir un stockage non volatil. Ce terme ne s'applique pas aux appareils de stockage qui sont un composant non remplaçable chez l'utilisateur d'une unité remplaçable chez l'utilisateur plus grande qui n'est pas principalement utilisée pour le stockage.
Pare-feu	Élément d'un système ou d'un réseau informatique conçu pour bloquer l'accès non autorisé tout en permettant les communications sortantes.
JOGF	Jour ouvrable du gouvernement fédéral
GC	Gouvernement du Canada

Terme	Définition
GIES du GC	Les produits logiciels et services de gestion de l'information et des événements de sécurité (GIES) combinent la gestion de la sécurité de l'information et la gestion des événements de sécurité. Ils fournissent une analyse en temps réel des alertes de sécurité générées par les applications et le matériel du réseau. Source : https://en.wikipedia.org/wiki/Security_information_and_event_management (en anglais)
Utilisateur général	Un utilisateur final qui n'est pas un utilisateur privilégié.
Frontières géographiques du Canada	Désigne tous les endroits au sein du Canada ainsi que les consulats et ambassades du Canada.
EFG	Équipement fourni par le gouvernement
Objet de stratégie de groupe (GPO)	Les objets de stratégie de groupe (Group Policy Object) sont une fonction de la famille de systèmes d'exploitation Microsoft Windows NT qui régissent l'environnement de travail des comptes utilisateurs et des comptes d'ordinateurs. Ils permettent, dans un environnement Active Directory, la gestion et la configuration centralisée des paramètres visant les systèmes d'exploitation, les applications et les utilisateurs. Source : https://en.wikipedia.org/wiki/Group_Policy (en anglais)
Renforcer la sécurité	Sécuriser un système en réduisant sa surface de vulnérabilité, qui est plus grande lorsqu'un système exécute plus de fonctions; en principe, un système à fonction unique est plus sûr qu'un système à fonctions multiples.
Matériel	Un appareil ou composant physique comme un ordinateur portable ou de bureau, une imprimante, un écran, un appareil de stockage physique, etc.
Identification	Une action ou un processus permettant d'identifier un utilisateur ou un appareil ou le fait d'être identifié.
Implémentation	Terme utilisé pour désigner les phases du cycle de vie du système qui sont responsables de la prestation d'un système d'information. Elle comprend les phases de lancement, de développement ou d'acquisition, d'intégration et d'installation du cycle de vie du système, mais exclut les phases d'exploitation, de maintenance et d'élimination.
Incident	Événement qui ne s'inscrit pas dans le cadre de fonctionnement normal d'un service et qui cause ou peut causer une interruption de service ou une réduction de la qualité du service.
Information (ressources d'information)	Suite de symboles ou de sons auxquels un sens peut être attribué. C'est ce qui informe. En d'autres termes, c'est la réponse à une question quelconque. Elle est donc liée aux données et aux connaissances, car les données représentent des valeurs attribuées à des paramètres, et la connaissance signifie la compréhension de choses réelles ou de concepts abstraits.
Système d'information	Un système d'information est habituellement constitué de données, de plateformes informatiques, de réseaux de communication, d'applications opérationnelles, de personnes et de processus organisés en vue de la collecte, du traitement, de l'actualisation, de l'utilisation, de l'échange, de la diffusion ou de l'élimination de l'information.

Terme	Définition
Infrastructure	Ensemble constitué du matériel, des logiciels et des réseaux nécessaires pour appuyer le service d'impression lié aux ATMT.
IP	Le protocole Internet (IP) est le principal protocole de communication de la suite de protocoles Internet pour transmettre des paquets à travers les limites des réseaux. Sa fonction d'acheminement permet l'interconnexion et crée essentiellement Internet. Source : https://en.wikipedia.org/wiki/Internet_Protocol (en anglais)
Intégrité	État de ce qui est précis, complet, authentique et intact. Remarque : L'intégrité s'applique généralement aux ressources d'information. L'intégrité peut aussi s'appliquer aux processus opérationnels, à la logique des applications logicielles, au matériel et au personnel.
Internet	Ensemble de serveurs de réseau et d'applications interconnectés et accessibles au grand public à l'échelle mondiale, communément appelé « Internet ».
Installation	Les services généraux d'installation fournis par l'entrepreneur.
TI	Technologie de l'information
Sécurité de la TI	Domaine dans lequel on met en œuvre des contrôles de sécurité, des solutions de sécurité, des outils et des techniques pour protéger les biens de TI contre les menaces de compromission tout au long de leur cycle de vie, selon la catégorie de sécurité des activités opérationnelles, et conformément aux politiques, directives, normes et lignes directrices du gouvernement du Canada.
Incident de sécurité de la TI	Tout événement imprévu ou indésirable compromettant ou susceptible de compromettre des biens de TI.
ITSG-06	Une méthode de nettoyage des données utilisant un logiciel servant à réécrire l'information existante.
ITSP.40.111	Les algorithmes cryptographiques pour les renseignements NON CLASSIFIÉS, de niveaux PROTÉGÉ A et PROTÉGÉ B sont une publication NON CLASSIFIÉE, publiée sous l'autorité du chef du Centre de la sécurité des télécommunications (CST). Source : https://www.cse-cst.gc.ca/fr/node/1831/html/26515
Travail	Tâche de traitement de documents soumise à l'appareil de copie. Une même tâche de traitement peut traiter un ou plusieurs documents.
NA3	Niveau d'assurance 3 - Réf : https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=26776
Réseau local (RL)	Réseau qui fournit une capacité de réseautage à un groupe d'ordinateurs situés à proximité les uns des autres.

Terme	Définition
Service de gestion d'impression	Il s'agit d'un service offert par un fournisseur externe pour optimiser ou gérer la production de documents d'une entreprise. Les principaux éléments fournis sont l'évaluation des besoins, le remplacement sélectif ou général du matériel, et le service, les pièces et les fournitures nécessaires à l'exploitation du nouveau matériel ou du matériel existant (y compris l'équipement existant de tiers si le client en a besoin). Le fournisseur assure également le suivi de la façon dont les imprimantes, les télécopieurs, les photocopieurs et les imprimantes multifonctions sont utilisés, des problèmes et de la satisfaction des utilisateurs. Il s'agit d'un ensemble de technologies, de services et de systèmes qui permettent d'améliorer la visibilité et le contrôle de l'environnement d'imagerie, ce qui se traduit par une meilleure productivité et des économies pour l'utilisateur final. Cela peut comprendre, sans s'y limiter, des composants de gestion des appareils d'impression, des outils de gestion des services et un portail de prestation de services.
Métadonnées	Données qui décrivent d'autres données.
AMF	Appareil multifonction
Surveillance	Il s'agit du processus continu d'observation des systèmes d'information dans le but de relever des écarts avec le comportement prévu ou planifié. Caractéristiques qui améliorent la productivité, par exemple : - Configurer à distance des appareils d'impression; - Gérer de nombreux appareils d'impression comme s'ils ne faisaient qu'un avec des fonctions de gestion par groupe; - Vérifier l'état des appareils d'impression dans toute l'entreprise; - Surveiller proactivement l'état des appareils d'impression en recevant des alertes sur l'état et les problèmes des appareils, ce qui permet de résoudre les problèmes quotidiens avant que les utilisateurs ne fassent l'expérience d'un temps d'arrêt; - Résoudre des problèmes. Caractéristiques qui réduisent les coûts, par exemple : - Suivi de l'utilisation des appareils d'impression par utilisateur final et par groupe afin de faciliter les politiques d'utilisation et de s'assurer que les appareils d'impression sont déployés de façon optimale dans l'organisation. Caractéristiques qui aident à assurer la sécurité, par exemple : Gérer et administrer de façon centralisée les paramètres importants de l'appareil d'impression pour garantir une mise en œuvre uniforme et adéquate des politiques et procédures de sécurité.
SGI	Service de gestion d'impression
Appareil multifonction (AMF)	Appareil d'impression qui imprime du contenu numérique sur papier, télécopie du contenu numérique sur une ligne téléphonique, numérise du contenu papier pour télécopier le contenu numérique sur une ligne téléphonique, numérise du contenu papier et le photocopie sur papier et numérise du contenu papier en contenu numérique.
Média non numérique	Tout média qui n'est pas numérisé. Par opposition avec les médias numériques.

Terme	Définition
Maintenance externe	Les activités de maintenance et de diagnostic externes sont les activités menées par des administrateurs ou des opérateurs qui communiquent par l'intermédiaire d'un réseau, soit un réseau externe (p. ex. Internet) ou un réseau interne. Les activités locales de maintenance et de diagnostic sont les activités effectuées par les administrateurs ou les opérateurs physiquement présents auprès du système d'information ou du composant du système d'information et qui ne communiquent pas avec une connexion réseau.
Opérateur	Une personne qui exploite le SGI et les systèmes. Les opérateurs peuvent avoir moins d'autorité que les administrateurs. Un opérateur s'occupe des besoins quotidiens du système. Cela pourrait comprendre le suivi des fournitures d'imprimante, des cartouches de bande de sauvegarde et d'autres éléments physiques communs. Le système envoie souvent des messages à un opérateur pour l'informer de problèmes d'imprimante ou de processus de sauvegarde, par exemple, et l'opérateur a la responsabilité de savoir comment traiter la demande et généralement de prendre les mesures nécessaires. Les messages comprennent aussi souvent des problèmes logiques plutôt que physiques. Les processus automatisés peuvent signaler des problèmes à un opérateur, et l'opérateur est responsable de savoir quelles sont les procédures de résolution de problèmes appropriées pour le site.
Imprimer	Un travail de conversion d'un document électronique en format papier.
Données d'impression	Les données relatives à un travail d'impression.
Appareil d'impression	Désigne une imprimante (réseau ou locale), un appareil multifonction, un photocopieur, un appareil de numérisation ou un télécopieur.
Tâche d'impression	Tâche de traitement de l'impression soumise à l'appareil de copie. Une même tâche de traitement peut traiter un ou plusieurs documents.
Imprimante	Un appareil d'impression qui imprime du contenu numérique sur papier.

Terme	Définition
Renseignements protégés	Les renseignements sont « protégés » si leur divulgation peut être préjudiciable à des intérêts autres que « l'intérêt national ». • Il y a trois niveaux de renseignements protégés : Protégé A (nature peu délicate) : s'applique aux renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer préjudice à des intérêts autres que l'intérêt national, par exemple, la divulgation du salaire exact. • Protégé B (nature particulièrement délicate) : s'applique à des renseignements pour lesquels toute atteinte à l'intégrité risquerait de causer de graves préjudices à des intérêts autres que l'intérêt national, par exemple, la perte de réputation ou d'un avantage concurrentiel. • Protégé C (nature extrêmement délicate) : s'applique à un nombre très restreint de renseignements pour lesquels toute atteinte à l'intégrité risquerait vraisemblablement de causer un préjudice extrêmement grave à des intérêts autres que l'intérêt national, par exemple, la perte de vie.
RTPC	Désigne le réseau téléphonique public commuté. Le RTPC est l'ensemble des réseaux téléphoniques mondiaux par commutation de circuit exploités par des opérateurs téléphoniques nationaux, régionaux ou locaux, qui fournissent une infrastructure et des services pour les télécommunications publiques.
Accès à distance	Accès à l'infrastructure du service de solution d'impression d'ATMT par l'entremise d'un réseau externe (p. ex. Internet).
Gestion à distance	Activités administratives ou de maintenance menées par un opérateur ou par un administrateur par l'entremise d'un réseau.
Risque	Se reporter à la définition de risque lié à la sécurité de la TI.
Salle	Un emplacement physique statique.
GRC	Gendarmerie royale du Canada
Contrôle d'accès fondé sur les rôles (RBAC)	Dans le domaine de la sécurité des systèmes informatiques, le contrôle d'accès basé sur les rôles (Roles Based Access Control) est une approche visant à restreindre l'accès au système aux utilisateurs autorisés. Il est utilisé par la majorité des entreprises de plus de 500 employés, et peut mettre en œuvre un contrôle d'accès obligatoire ou discrétionnaire. Le RBAC est parfois appelé sécurité axée sur les rôles. Source : https://en.wikipedia.org/wiki/Role-based_access_control (en anglais)

Terme	Définition
Évaluations de sécurité	Processus continu d'évaluation du rendement des contrôles de sécurité de TI pendant le cycle de vie des systèmes d'information. Ce processus vise à établir la mesure dans laquelle les contrôles sont mis en œuvre adéquatement, fonctionnent comme prévu, et produisent les résultats voulus pour ce qui est de répondre aux besoins opérationnels des ministères en matière de sécurité. L'évaluation de la sécurité appuie l'autorisation en fournissant les raisons pour lesquelles la confiance à l'égard de la sécurité du système d'information est justifiée.
Évaluation de sécurité et autorisation (ESA)	Processus continu d'évaluation du rendement des contrôles de sécurité de TI pendant le cycle de vie des systèmes d'information. Ce processus vise à établir la mesure dans laquelle les contrôles sont mis en œuvre adéquatement, fonctionnent comme prévu, et produisent les résultats voulus pour ce qui est de répondre aux besoins opérationnels des ministères en matière de sécurité. L'évaluation de la sécurité appuie l'autorisation en fournissant les raisons pour lesquelles la confiance à l'égard de la sécurité du système d'information est justifiée.
Contrôle de sécurité	Exigence de haut niveau technique, opérationnelle ou de gestion relative à la sécurité et prescrite pour un système d'information afin de protéger la confidentialité, l'intégrité et la disponibilité de ses biens de TI. Les contrôles de sécurité sont mis en œuvre par l'application de différents types de solutions de sécurité qui comprennent les produits, les politiques, les pratiques et les procédures de sécurité.
Incident de sécurité	Comportement ou événement non autorisé (contrevenant à la politique de sécurité du système de TI) relatif à l'exploitation et à l'administration du système informatique pouvant potentiellement compromettre la confidentialité, l'intégrité ou la disponibilité du système informatique.
Gestion de l'information et des événements de sécurité (GIES)	Une technologie qui permet une analyse en temps réel (collecte, agrégation, corrélation) d'alertes de sécurité générées par les composants et les applications de l'infrastructure.
Posture de sécurité	Caractéristique d'un système d'information qui représente sa résilience face aux menaces, aux vulnérabilités, à un ensemble précis d'attaques délibérées ainsi qu'aux risques accidentels et naturels. Remarque : La résilience ne concerne pas seulement la capacité du système d'information à prévenir les menaces, mais aussi à détecter, à réagir et à se remettre des compromissions.
Exigence relative à la sécurité	Tout besoin, exprimé dans un langage normalisé, qu'un système d'information doit satisfaire grâce à ses mesures de sécurité de la TI et qui contribue à répondre à un besoin opérationnel de sécurité.
Liste de vérification des exigences relatives à la sécurité (LVERS)	Exigences en matière d'habilitation du personnel, des installations et de l'organisation.
Point de prestation de services (PPS)	Un étage ou une salle dans un bâtiment où un service ou produit d'impression lié aux ATMT est mis en œuvre.
Portail de prestation de services	Désigne le portail de services fourni et géré par le fournisseur de services.

Terme	Définition
Données de gestion des services	Les données issues de l'exploitation, de l'administration et de la gestion des services de soutien et de la facturation : a) les demandes de service; b) les dossiers d'incident (à l'exception des dossiers d'incident de sécurité); c) les documents de facturation et les factures à l'échelle de l'organisation; d) les dossiers sur les biens; e) les dossiers sur la configuration; f) les données sur la performance du système, la capacité et la planification des ressources; g) des détails sur l'état des appareils, les codes d'erreur et les événements.
Fournisseur de service	Une entité responsable de la prestation du service aux clients.
GIES	Gestion de l'information et des événements de sécurité
Site	Une installation d'un seul étage ou un étage dans une installation à plusieurs étages.
Carte à puce	Un petit appareil électronique de la taille d'une carte de crédit qui contient une mémoire électronique et qui est utilisé à diverses fins, comme l'authentification de l'identité d'un utilisateur.
Logiciel	Une application utilisée par un utilisateur final. Un logiciel est habituellement installé sur du matériel.
LVERS	Liste de vérification des exigences relatives à la sécurité
SPC	Services partagés Canada
X	Tests et évaluation de la sécurité
Système	Terme générique désignant le réseau et d'autres appareils, les systèmes d'exploitation, les plateformes, les logiciels de virtualisation ou toute combinaison de ces éléments. Son utilisation est propre à un contexte.
Données du système	Données que l'entrepreneur utilise pour contrôler ou modifier le fonctionnement, l'administration et la gestion des services d'impression liés aux ATMT, ce qui comprend : a) les incidents de sécurité; b) la gestion de l'information et des événements de sécurité; c) la gestion du périmètre du réseau (p. ex. pare-feu); d) la gestion des intrusions et de la prévention; e) la protection contre les logiciels malveillants et les renseignements relatifs aux contrôles de sécurité; f) la gestion de l'hyperviseur et des systèmes de la machine virtuelle; g) la gestion du réseau et les opérations; h) les fichiers, les registres et les scripts relatifs à la configuration du système; i) les systèmes d'authentification, d'autorisation et de comptabilité; j) les systèmes à disques; k) les systèmes de gestion des ressources et de la capacité; l) la distribution, les mises à jour et les correctifs des logiciels; m) les services d'annuaire.
Menace	Se reporter à la définition de menace pour les TI. Fait référence à tout événement, acte ou danger éventuel, délibéré, accidentel ou naturel qui pourrait mettre en péril les biens de TI.

Terme	Définition
Accès non autorisé	Lorsqu'une entité obtient un accès non autorisé à un système. Cela peut consister notamment en une infiltration, une compromission, un piratage, une élévation des privilèges ou en l'obtention non autorisée d'un accès ou privilège.
Personnes non autorisées	Toute personne qui n'est pas autorisée à avoir accès à certains systèmes, biens, emplacements, renseignements, etc.
Utilisateur	Un agent, qu'il s'agisse d'un agent humain (utilisateur final) ou d'un agent logiciel, qui utilise un service informatique ou réseau.
Données de l'utilisateur	Les données relatives aux documents et dossiers d'utilisateur qui sont numérisés, télécopiés et imprimés, ainsi que les données de compte et de répertoire connexes de l'utilisateur.
Vulnérabilité	Caractéristiques d'un bien ou de son environnement (y compris la solution de sécurité) qui rendent ce bien plus susceptible d'être compromis, qui augmentent la probabilité d'occurrence d'une menace ou la gravité des effets de celle-ci.
Évaluation de la vulnérabilité	Détermination de l'existence des vulnérabilités d'un système d'information.
Réseau sans fil	Tout type de réseau informatique qui utilise des connexions de données sans fil pour connecter les nœuds du réseau.
Appareils technologiques en milieu de travail (ATMT)	Une direction générale de Services partagés Canada. Son objectif est de normaliser et regrouper l'acquisition et l'approvisionnement du matériel et des logiciels destinés aux appareils technologiques en milieu de travail du gouvernement du Canada.