Centre de la sécurité des télécommunications
Communications Security Establishment

NON CLASSIFIÉ

SÉRIE GESTIONNAIRES

CONSEILS EN MATIÈRE DE SÉCURITÉ DES TECHNOLOGIES DE L'INFORMATION

SÉCURISATION DE L'ENTREPRISE ET DES TECHNOLOGIES MOBILES

ITSM.80.001

Juillet 2016

Canada

INTRODUCTION

Les dispositifs mobiles jouent un rôle essentiel dans les ministères et organismes du gouvernement du Canada (GC), et ont déjà été adoptés par la majorité au sein de la fonction publique. Les dispositifs mobiles, notamment les téléphones dits intelligents, les tablettes et les ordinateurs portables, offrent de puissantes fonctionnalités de traitement de l'information et sont en mesure de communiquer avec d'autres dispositifs grâce aux technologies sans fil, cellulaires et Bluetooth. Pour les employés du GC, le recours aux fonctions étendues de ces appareils permet notamment de remplacer le papier, de prendre des notes pendant les réunions ou de lire des documents en cours de déplacement.

Les dispositifs mobiles sont devenus de puissants facilitateurs de collaboration et, bien qu'ils puissent constituer d'importants facteurs de productivité et d'efficacité, ils n'en augmentent pas moins les risques de compromission de l'information sensible du GC. Les risques pour la sécurité sont nombreux, et il faut les évaluer avec soin, s'assurer de bien les comprendre, et mettre en place des contrôles de sécurité et des mesures de protection avant d'autoriser tout accès à un réseau ministériel par des dispositifs mobiles.

Le présent document brosse un tableau de la sécurité mobile d'entreprise et fait état des menaces et des risques que les dispositifs mobiles posent à l'environnement des ministères du GC. Il propose également une synthèse des mesures d'atténuation et de protection qu'un ministère peut mettre en œuvre pour contrer les menaces et atténuer les risques. Il importe de souligner que cette liste n'est pas exhaustive et que même dans une situation où toutes les stratégies d'atténuation potentielles auraient été correctement mises en place, il existerait toujours un risque résiduel pour le réseau et les biens d'information du ministère.

FACTEURS POLITIQUES

Dans l'environnement réseau du GC, l'analyse des menaces, des risques et des vulnérabilités ainsi que les mesures de prévention et de protection sont des facteurs essentiels à la sécurisation des structures de communication, des données et des actifs dont le GC est responsable. Par conséquent, les ministères du GC doivent veiller à ce que les politiques et les procédures en matière de sécurité des TI soient mises en œuvre conformément aux politiques du Secrétariat du Conseil du Trésor (SCT) du Canada.

- *Politique sur la gestion des technologies de l'information* [1][1];
- *Politique sur la sécurité du gouvernement* [2];
- *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information* (GSTI) [3]

ENVIRONNEMENTS CONCERNÉS

La présente contient notamment des conseils en matière de TI pour les environnements NON CLASSIFIÉ, PROTÉGÉ A et PREOTÉGÉ B. Les systèmes utilisés dans les domaines PROTÉGÉ C ou classifiés pourraient nécessiter des mesures additionnelles qui ne sont pas abordées dans le présent document[2]. Conformément à

[1] Les numéros entre les crochets renvoient à des éléments de référence figurant à la section *Contenu complémentaire* du présent document.

[2] Pour obtenir des conseils en matière de TI pour les domaines PROTÉGÉ C ou classifiés, prière de communiquer avec les Services à la clientèle en matière de COMSEC.

leurs cadres respectifs de gestion des risques, les ministères sont tenus de définir des objectifs de sécurité qui soient propices à la protection des informations et des services ministériels.

MOBILITÉ ET ENTREPRISE : FACTEURS OPÉRATIONNELS

Les employés du GC constituent un effectif de classe mondiale qui doit compter sur les technologies de pointe pour exécuter les tâches qui leur incombent et veiller à ce que les ministères réalisent leurs objectifs. Par conséquent, le nombre des employés qui ont recours aux technologies mobiles ne cesse d'augmenter, principalement pour les motifs suivants.

- **Convivialité –** Les dispositifs mobiles sont dotés d'interfaces conviviales personnalisables et peuvent ainsi combler les besoins à la fois des employés et du GC.
- **Connectivité en tout temps et en tout lieu** – Les employés du GC doivent disposer d'un accès à distance aux données ainsi qu'aux services et applications d'entreprise pour être en mesure de travailler efficacement. Cette exigence concerne au premier chef les employés du GC qui se déplacent fréquemment.
- **Personnalisation** – Les ministères ont la possibilité de personnaliser les paramètres des dispositifs de façon à rendre ceux-ci plus pratiques et conviviaux pour les employés qui les utilisent.
- **Infonuagique** – Le GC exploite de plus en plus les infrastructures d'infonuagique pour prodiguer ses services.
- **Coût pour le GC** – Les fournisseurs de dispositifs mobiles ne cessent d'accroître la qualité et la puissance de leurs appareils. Le recours aux dispositifs mobiles et aux fournisseurs de services contribue à réduire les coûts de programme et élimine les problèmes liés à la désuétude des technologies, des avantages que le ne retrouve pas avec les solutions définies et conçues par le GC.

MOBILITÉ ET ENTREPRISE : APERÇU

Dans les divers ministères, la mobilité permet aux employés d'accéder à des données et à des services ministériels peu importe le lieu ou l'heure – qu'ils se trouvent dans leur édifice, dans leur ville, dans leur pays ou à l'étranger. L'accès aux réseaux éloignés que procurent les dispositifs mobiles permet aux employés de collaborer entre eux et d'exécuter leurs tâches respectives tout en maintenant un niveau d'efficacité adéquat.

Les technologies mobiles pour entreprises permettent aux dispositifs comme les téléphones intelligents, les tablettes et les ordinateurs portatifs de se connecter aux réseaux et services des ministères grâce aux solutions commerciales d'accès réseau cellulaires et sans fil. La figure 1 illustre la façon dont s'articulent les divers éléments d'une architecture de mobilité d'entreprise.

Figure 1 Organisation des divers éléments d'une architecture de mobilité d'entreprise

DISPOSITIFS MOBILES

Les dispositifs mobiles sont des produits commerciaux – comme les téléphones intelligents, les téléphones polyvalents, les tablettes électroniques, et les ordinateurs portables – qui sont aptes à se connecter aux réseaux du GC. Les dispositifs mobiles dont disponibles partout, ils sont abordables et sont dotés des dernières technologies de communication et des plus récentes applications. Les fonctions des dispositifs mobiles évoluent constamment, mais ces derniers offrent généralement une gamme commune de fonctions, notamment la connexion réseau, la communication de données de renseignements et de données vocales, le stockage des données, la géolocalisation GPS, l'appareil photo et la caméra vidéo.

RÉSEAUX DE COMMUNICATION SANS FIL

Principaux types de réseaux sans fil :

- **Réseau cellulaire** – administrés par les entreprises de télécommunications; la superficie de leurs zones de couverture respectives résulte de la subdivision de vastes zones de service.
- **Réseau sans fil** – peut être établi par des entreprises ou des particuliers, dans le but d'offrir un service réseau à l'intérieur d'une zone définie, qu'il s'agisse, par exemple, du domicile, du bureau ou d'une zone de travail.
- **Autres types de réseaux sans fil** – technologies pouvant ne pas être conformes aux normes régissant les communications sans fil. Par exemple, la technologie Bluetooth est fréquemment utilisée pour interconnecter des dispositifs qui sont à courte distance les uns des autres, notamment les casques d'écoute ou les claviers d'ordinateur.

INFRASTRUCTURE D'ENTREPRISE DU GC

L'infrastructure d'entreprise du GC fournit le matériel, les logiciels, les ressources réseau et les services qui sont essentiels à la création, à l'exploitation et à la gestion d'un environnement de TI d'entreprise. En l'occurrence, le GC est en mesure de prodiguer des solutions et des services de TI à ses employés, à ses partenaires ainsi qu'à ses clients. Les applications ayant trait particulièrement à la mobilité peuvent également être hébergées dans l'environnement d'entreprise du GC, mais la possibilité de communiquer avec d'autres dispositifs mobiles peut

également être offerte. Les capacités en matière de mobilité d'entreprise permettent la sécurisation et la gestion des interactions entre les services d'entreprise du GC, d'une part, et les dispositifs et utilisateurs autorisés, d'autre part.

SERVICES ET APPLICATIONS

Les services et les applications consistent en des services évolutifs qui sont déjà fournis à l'ensemble des utilisateurs de l'environnement d'entreprise, y compris aux utilisateurs des technologies mobiles. Les services d'entreprise du GC comprennent les communications unifiées, à savoir les données de renseignement (courriel et clavardage) et les données vocales (téléphone et téléconférence), ainsi que les applications et les interfaces Web.

GESTION DES RISQUES EN MATIÈRE DE SÉCURITÉ DES TI

Par ailleurs, l'utilisation des dispositifs mobiles, des réseaux sans fil, et des services de données et de voix expose le GC à un certain nombre de menaces. Ces menaces peuvent découler d'accidents ou d'actes délibérés et peuvent être le fait d'utilisateurs autorisés tout autant que d'adversaires. Elles doivent donc être contrées ou suffisamment atténuées pour atteindre des niveaux de risque qui soient acceptables. Il existe un certain nombre de mesures d'atténuation qui visent les menaces pesant sur les technologies mobiles, et la majeure partie d'entre elles fonctionnent de concert, les unes avec les autres. Plus particulièrement, l'infrastructure d'entreprise relative à la mobilité de même que les capacités d'entreprise déjà existantes offrent des mesures de sécurité qui pourront protéger adéquatement les dispositifs mobiles et les communications des employés.

MENACES ET RISQUES

Les dispositifs mobiles doivent souvent être l'objet d'une protection accrue, puisque les fonctions qui les caractérisent les exposent davantage aux menaces que les autres types de dispositifs clients (contrairement aux ordinateurs de bureau et aux ordinateurs portables qui sont utilisés exclusivement dans l'enceinte de l'organisme ou dans les réseaux organisationnels). Voici une liste des principaux enjeux en matière de sécurité :

- lacunes sur le plan des contrôles de sécurité;
- emploi de dispositifs mobiles jugés non fiables;
- utilisation de réseaux non fiables;
- utilisation d'applications non fiables;
- interaction avec d'autres systèmes;
- utilisation de contenus non fiables;
- recours à des dispositifs de location.

Il conviendra donc de bien connaître et d'atténuer adéquatement les nombreuses menaces auxquelles s'exposent les dispositifs mobiles, ce qui permettra de garantir la confidentialité, la disponibilité et l'intégrité des informations du GC. Voici les principales menaces sur lesquelles il conviendra de se concentrer.

MENACES ET RISQUES LIÉS AUX DISPOSITIFS

- Identification, ciblage et transmission de maliciels visant des dispositifs.
- Utilisation des connexions réseau des dispositifs (cellulaire, sans-fil, Bluetooth) à des fins malveillantes.

- Utilisation de dispositifs pour infiltrer d'autres réseaux du GC.
- Accès à des dispositifs dans le but de surveiller les déplacements au moyen de la localisation GPS.
- Activation d'un micro ou d'une caméra.
- Interception de communications contenant des données de renseignement ou des données vocales.
- Accès, par le logiciel d'une tierce partie, aux fonctionnalités des dispositifs.
- Modification non autorisée des dispositifs, notamment les changements de composantes matérielles ou logicielles d'un dispositif mobile, qui sont exécutés à distance, directement sur l'appareil ou en quelque lieu de la chaîne d'approvisionnement.
- Défauts logiciels, systèmes d'exploitation désuets.

MENACES ET RISQUES VISANT LA CONFIDENTIALITÉ, L'INTÉGRITÉ ET LA DISPONIBILITÉ DE L'INFORMATION

- Exfiltration ou surveillance des communications (voix ou données) transmises par les technologies Bluetooth ou sans fil ou encore par d'autres moyens.
- Données sensibles stockées sans protection dans un dispositif mobile.
- Attaques par déni de service.

MENACES ET RISQUES POUR L'ENTREPRISE

- Perte d'éléments d'authentification comme les mots de passe ou les clés privées pour certificats.
- Élimination inadéquate de vieux dispositifs mobiles dotés de configurations ou de données sensibles.
- Usage interdit (par les politiques) de médias sociaux.
- Dispositifs perdus ou volés par lesquels on tente d'accéder à l'infrastructure de mobilité d'entreprise ou d'usurper l'identité d'utilisateurs autorisés.
- Personnes autorisées à utiliser l'équipement qui, en revanche, abusent de leurs privilèges en tentant, notamment, d'utiliser des services ou des applications pour lesquels elles n'ont pas les droits requis, ou de se connecter directement à des services commerciaux.
- Les boutiques non fiables qui insèrent des maliciels dans des logiciels populaires avant de redistribuer ces derniers.

PROCESSUS DE GESTION DES RISQUES EN SÉCURITÉ DES TI

Les lignes directrices du document *Gestion des risques liés à la sécurité des TI – Une méthode axée sur le cycle de vie* (ITSG-33) propose un ensemble d'activités pour chacun des deux niveaux organisationnels suivants : le niveau ministériel et le niveau des systèmes d'information. Les activités du niveau ministériel sont intégrées au programme de sécurité de l'organisation pour planifier, gérer, évaluer et améliorer la gestion des risques liés à la sécurité des TI. Après avoir défini l'ensemble des rôles et responsabilités, les lignes directrices à l'Annexe 1 du guide ITSG-33 [4] proposent et décrivent des activités de gestion des risques liés à la sécurité des TI qui permettent de définir, de déployer, de surveiller, d'évaluer et de mettre à jour les contrôles de sécurité à l'échelle du ministère. La mise en œuvre de ces activités suit un cycle de vie standard qui doit être intégré au programme global de sécurité ministérielle.

Quant aux activités du niveau des systèmes d'information, elles sont intégrées au cycle de vie des systèmes d'information pour s'assurer de répondre aux besoins en matière de sécurité des TI des activités opérationnelles prises en charge et pour veiller à ce que les contrôles de sécurité appropriés soient mis en œuvre et exploités comme prévu, à ce que le rendement des contrôles existants soit évalué en permanence et fasse l'objet de rapports, et à ce que des mesures appropriées soient prises pour corriger toute lacune relevée. Les lignes directrices de l'Annexe 2 du guide ITSG-33 [4] proposent des activités de gestion des risques liés à la sécurité des TI pour mettre en œuvre, exploiter et maintenir des systèmes d'information fiables. Ces activités s'appliquent au cycle de vie des systèmes d'information, qui inclut les phases de mise en œuvre, d'exploitation et de maintenance, et d'élimination. Pour aider les ministères, l'Annexe 2 du guide ITSG-33 [4] propose un processus de cycle de développement des systèmes (CDS) sécurisé appelé processus d'application de la sécurité dans les systèmes d'information (PASSI).

STRATÉGIE D'ATTÉNUATION

Les ministères devraient mettre en œuvre une stratégie de défense exhaustive qui comptera une multiplicité de strates de sécurité établies dans tout le système de TI, de façon à offrir un degré de redondance permettant de réagir adéquatement en cas de défaillance des contrôles de sécurité et d'exploitation des vulnérabilités. Pour être en mesure de protéger les informations sensibles et les réseaux du GC, les ministères devraient mettre en œuvre, tel qu'il est indiqué ci-dessous, ladite stratégie en profondeur axée sur la stratification des moyens de sécurité. La stratégie comporte trois strates de sécurité, lesquelles se concentrent à parts égales sur trois éléments centraux : les personnes, les technologies et les opérations.

1. LES MINISTÈRES DEVRAIENT SE DOTER D'UNE POLITIQUE SUR LA SÉCURITÉ DES DISPOSITIFS MOBILES

La politique ministérielle sur la sécurité des dispositifs mobiles devrait définir les ressources qui pourront être accessibles aux dispositifs mobiles, le degré d'accès dont ces dispositifs peuvent disposer, et les types de dispositifs qui seront autorisés à accéder aux ressources ministérielles (p. ex. les dispositifs distribués par le GC par opposition aux dispositifs personnels). Ladite politique devrait également porter sur la façon dont les serveurs de gestion des dispositifs mobiles doivent être administrés, sur le processus de mise à jour de ladite politique, et sur les exigences s'appliquant aux technologies de gestion des dispositifs mobiles. La politique sur la sécurité des dispositifs mobiles devrait être documentée dans le plan ministériel de sécurité.

2. LES MINISTÈRES DEVRAIENT METTRE EN ŒUVRE UN PROGRAMME DE FORMATION ET DE SENSIBILISATION DES EMPLOYÉS

La sécurité de l'information, c'est l'affaire de tout le personnel de l'organisme. La responsabilité des employés doit être clairement définie, communiquée et soutenue par une formation et une sensibilisation efficaces. Il suffit d'ouvrir une seule pièce jointe dans un courriel piraté ou d'accéder à un seul site Web malveillant pour compromettre l'ensemble d'un réseau. La continuité des activités dans le contexte actuel de cybermenace repose essentiellement sur la rigueur et l'engagement des employés. Il est donc impératif que la haute direction mise sur la sensibilisation et que celle-ci soit intégrée au cadre stratégique.

3. LES MINISTÈRES DEVRAIENT PROCÉDER À DES ÉVALUATIONS DE MENACES ET DE RISQUES VISANT L'UTILISATION DES DISPOSITIFS MOBILES

Les dispositifs mobiles doivent souvent être l'objet d'une protection accrue, puisque les fonctions qui les caractérisent les exposent davantage aux menaces que les autres types de dispositifs. Avant de concevoir et de mettre en œuvre des solutions visant les dispositifs mobiles, les ministères devraient procéder à des évaluations

de menaces et de risques (EMR). Les EMR permettent aux ministères de définir les exigences en matière de sécurité et d'élaborer des solutions destinées aux dispositifs mobiles, lesquelles comprendront des contrôles de sécurité répondant auxdites exigences. En cours d'EMR, on dresse un portrait des ressources d'intérêt, des menaces et vulnérabilités liées à ces ressources ainsi que des contrôles de sécurité qui s'imposent en l'occurrence; ensuite, on calcule les probabilités de réussite et les éventuelles répercussions des attaques; et enfin, on analyse l'information produite de façon à savoir quels contrôles de sécurité il faut ajouter ou perfectionner.

4. LES MINISTÈRES DEVRAIENT VEILLER À CE QUE LES SERVICES DE SÉCURITÉ REQUIS SOIENT MIS À CONTRIBUTION

Les ministères devraient analyser la pertinence de chacun des services pour ensuite hiérarchiser ceux-ci de façon à pouvoir mettre en œuvre les solutions les plus appropriées. Les services à prendre en compte sont les suivants :

- **Politique ministérielle sur la sécurité :** application des politiques ministérielles portant sur les dispositifs mobiles, notamment en matière de restriction des accès au matériel et aux logiciels; de gestion des interfaces de réseau sans fil; d'automatisation des moyens de surveillance et de détection; et de production de rapports en cas d'infraction aux dispositions de la politique.
- **Transmission et stockage des données :** favoriser le chiffrement fort des transmissions de données et du stockage de données, ne remettre les dispositifs à de nouveaux utilisateurs qu'après en avoir supprimé les données, et supprimer à distance les données des dispositifs ayant été volés ou perdus.
- **Authentification des dispositifs et des utilisateurs :** exiger l'authentification des dispositifs avant de permettre aux dispositifs mobiles de se connecter aux ressources du ministère.
- **Applications de tierces parties :** établissement de la liste des applications pouvant être installées, définition des autorisations d'accès pour chacune des applications et vérification des signatures numériques des applications.

5. LES MINISTÈRES DEVRAIENT SOUMETTRE À DES ESSAIS PILOTES LES SOLUTIONS VISANT LES DISPOSITIFS MOBILES

Certains aspects de la solution devraient être évalués pour chaque type de dispositifs mobiles, notamment la connectivité, la protection, l'authentification, la fonctionnalité des applications, la gestion des solutions, la journalisation et la performance. Toutes les composantes du système devraient recevoir les plus récents correctifs et être configurées conformément aux pratiques exemplaires en matière de sécurité.

6. LES MINISTÈRES DEVRAIENT SÉCURISER LES DISPOSITIFS MOBILES AVANT DE DÉFINIR LES DROITS D'ACCÈS DES UTILISATEURS

Le fait de sécuriser chacun des dispositifs avant de permettre aux utilisateurs de s'en servir garantit un certain niveau de fiabilité des dispositifs en question avant qu'ils ne soient de facto exposés aux menaces. Tout dispositif mobile du GC qui a déjà été attribué et dont les profils de sécurité sont inconnus devrait être intégralement sécurisé et ramené à un état de fonctionnement acceptable au moyen des technologies de gestion des dispositifs mobiles. Des contrôles de sécurité additionnels devraient être appliqués en fonction des risques, notamment les logiciels antivirus et les technologies de prévention des pertes de données (DLP pour *Data-Loss Prevention*).

7. LES MINISTÈRES DEVRAIENT OBSERVER UN CALENDRIER DE MAINTENANCE DE LA SÉCURITÉ DES DISPOSITIFS MOBILES

Les processus ministériels en matière de maintenance de la sécurité comptent les éléments suivants.

- Veiller à ce que les mises à niveau et les correctifs soient installés en temps opportun.
- Reconfigurer les paramètres des contrôles d'accès, s'il y a lieu.
- Détecter et enregistrer les anomalies observées dans l'infrastructure des dispositifs mobiles, y compris les modifications non autorisées qui auraient été apportées à la configuration des dispositifs mobiles.
- Tenir un inventaire à jour des dispositifs mobiles et des applications connexes.
- Révoquer les accès ou supprimer les applications qui constituent un risque excessif.
- Supprimer intégralement les données sensibles des dispositifs mobiles avant de réattribuer ceux-ci à de nouveaux utilisateurs.

Les ministères devraient procéder périodiquement à des vérifications qui permettront de s'assurer que les politiques, les processus et les procédures en vigueur ont été respectés.

SÉRIE DU CST SUR LA MOBILITÉ

Pour stimuler la résistance aux menaces qui visent les dispositifs mobiles, le CST a préparé une série de publications faisant état de pratiques qui permettront aux ministères du GC de réduire considérablement l'exposition des dispositifs mobiles auxdites menaces. Prière d'utiliser ce lien www.cse-cst.gc.ca/fr/its pour télécharger la documentation suivante :

- Technologies mobiles pour les voyages internationaux
- Les 10 mesures de sécurité du CST
- Solutions de gestion de dispositifs mobiles (MDM pour *Mobile Device Management*)
- La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie
- Exigences de sécurité liées aux réseaux locaux sans fil
- Répercussions sur la sécurité de l'exposition de systèmes TI classifiés à des dispositifs mobiles et à des signaux sans fil
- Sécurité mobile : accès, en tout temps, en tout lieu
- Utiliser son dispositif mobile en toute sécurité

SOMMAIRE

Les dispositifs mobiles sont pratiques et polyvalents, et ils permettent aux employés de travailler en tout temps et en tout lieu. En revanche, leur facture complexe et les fonctions élaborées qu'ils offrent constituent des facteurs de risque pour les informations, les actifs et les réseaux du GC. Ces dispositifs permettent de stocker ou de consulter à distance d'importantes quantités de renseignements personnels et gouvernementaux sensibles, ce qui en fait des cibles de premier plan pour les auteurs de menaces qui cherchent à recueillir de l'information.

Les dispositifs mobiles disponibles dans le commerce ne répondent pas à toutes les exigences de sécurité qu'il convient de respecter dans les activités du GC. Il faut donc bien connaître et atténuer adéquatement les nombreuses menaces auxquelles s'exposent les dispositifs mobiles, ce qui permettra de garantir la confidentialité, la disponibilité et l'intégrité des informations du GC. Les technologies mobiles pour entreprises devraient commencer avec les mesures de protection offertes dans le marché, pour ensuite pallier les lacunes inhérentes aux dispositifs. Il conviendra également de tirer parti de l'intégration de la sécurité au GC et d'élaborer des politiques de sécurité portant exclusivement sur les dispositifs mobiles. S'il y a lieu, les dispositifs mobiles commerciaux peuvent être renforcés de façon à en garantir l'intégrité et à atténuer les risques.

Certes, les technologies mobiles sont devenues une nécessité pour les employés du GC, mais il va de soi que la confidentialité, la disponibilité et l'intégrité de l'information doivent absolument être garanties. Par conséquent, les contrôles de sécurité s'appliquant aux solutions du GC en matière de mobilité d'entreprise devraient être établis suivant une évaluation ministérielle des menaces et des risques. L'ITSG-33 – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, une publication du CST, décrit un processus de gestion des risques de sécurité en vertu duquel on peut personnaliser des contrôles de sécurité courants, de manière à répondre aux besoins particuliers d'un ministère en matière de sécurité. Les contrôles de sécurité doivent être instaurés et vérifiés pour l'ensemble du système d'information, et ce, du dispositif mobile individuel jusqu'aux services de réseau du ministère, pour permettre l'application des processus opérationnels et l'intégrité des biens d'information.

AIDE ET RENSEIGNEMENTS

Si les représentants de votre ministère ont identifié des besoins en matière de mobilité et souhaitent obtenir de plus amples renseignements, veuillez communiquer avec les Services à la clientèle de la STI du CST :

Services à la clientèle de la STI
Téléphone : 613-991-7654
Courriel : itsclientservices@cse-cst.gc.ca

CONTENU COMPLÉMENTAIRE

LISTE D'ABRÉVIATIONS, D'ACRONYMES ET DE SIGLES

Terme	Définition
CDS	Cycle de développement des systèmes
CST	Centre de la sécurité des télécommunications
DLP	Prévention des pertes de données (*Data Loss Prevention*)
GC	Gouvernement du Canada
GPS	Localisation GPS (*Global Positioning Systems*)
PASSI	Processus d'application de la sécurité dans les systèmes d'information
SCT	Secrétariat du Conseil du Trésor
STI	Sécurité des technologies de l'information
TI	Technologies de l'information

RÉFÉRENCES

Numéro	Référence
1	Secrétariat du Conseil du Trésor. *Politique sur la gestion des technologies de l'information*, 1er juillet 2007.
2	Secrétariat du Conseil du Trésor. *Politique sur la sécurité du gouvernement* (PSG), 1er juillet 2009
3	Secrétariat du Conseil du Trésor. *Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information*, sans date.
4	Centre de la sécurité des télécommunications. ITSG-33 – *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014
5	National Security Agency. *Mobility Security Guide*, 4 novembre 2013.
6	National Institute of Standards and Technology. Special Publication 800-124, Revision 1

	Guidelines for Managing the Security of Mobile Devices in the Enterprise, juin 2013.
7	United States Government Accountability Office. *Better Implementation of Controls for Mobile Devices Should Be Encouraged*, septembre 2012.
8	United States Computer Emergency Readiness Team. *Technical Information Paper-TIP-10-105-01 Cyber Threats to Mobile Devices*, 15 avril 2010.