Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CONSEILS SUR LE RENFORCEMENT DE LA SÉCURITÉ DE MICROSOFT WINDOWS 10 ENTERPRISE

ITSP.70.012

Mars 2019

SÉRIE PRATICIENS

Canada

AVANT-PROPOS

Le document ITSP.70.012 Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise est NON CLASSIFIÉ, et il est publié avec l'autorisation du chef du Centre de la sécurité des télécommunications (CST). Pour de plus amples renseignements ou pour des suggestions de modifications, prière de communiquer avec l'équipe des Services à la clientèle du Centre canadien pour la cybersécurité (CCC) :

Centre d'appels
contact@cyber.gc.ca
613-949-7048 ou 1-833-CYBER-88

DATE D'ENTRÉE EN VIGUEUR

Le présent document entre en vigueur le (01/03/2018).

APERÇU

Le présent document offre des conseils techniques sur les outils et les fonctions de sécurité de Microsoft qu'il est possible d'utiliser pour renforcer la sécurité des systèmes d'exploitation Windows 10 Enterprise (« Windows 10 »). Il fait mention de certaines solutions de contournement reconnues et de certains correctifs apportés à des problèmes de sécurité connus dans Windows 10. Ce document introduit également les configurations de référence associées aux paramètres des objets de stratégies de groupe (GPO pour *Group Policy Object*). Les paramètres de GPO sont expliqués dans une annexe qu'il est possible de se procurer auprès du Centre d'appels du CCC. Les instructions pour obtenir une copie des paramètres de GPO [1] se trouvent à la section 8.1 de ce document.

Windows 10 est un système d'exploitation communément utilisé sur les ordinateurs de bureau. Bien que le présent document ait été essentiellement rédigé à l'intention des ministères du gouvernement du Canada (GC), les organismes qui ne font pas partie du GC peuvent également mettre en pratique les recommandations qu'il contient.

Les outils et les fonctions de sécurité mentionnés constituaient les plus récents services offerts par Microsoft pour Windows 10 (version 1607) au moment de publier le présent document. Ce dernier pourrait être mis à jour de manière à faire mention de l'ensemble des outils et des fonctions de sécurité pertinents. Les paramètres de GPO seront également mis à jour pour tenir compte des versions semestrielles de Microsoft.

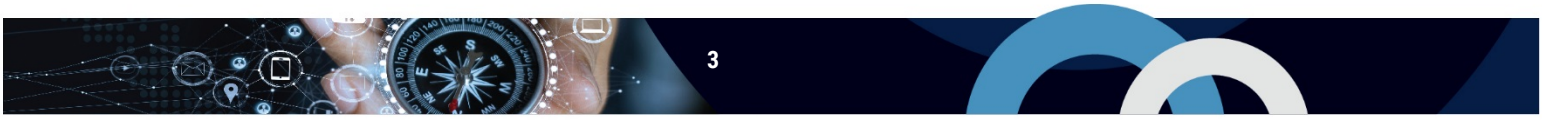

TABLE DES MATIÈRES

LISTE DES FIGURES

LISTE DES TABLEAUX

1 INTRODUCTION

Pour prévenir la compromission des systèmes de technologies de l'information (TI) et des réseaux, l'une des 10 principales mesures de sécurité recommandées est de renforcer la sécurité des systèmes d'exploitation (pour plus de détails à ce sujet, voir *l'ITSM.10.189 – Les 10 meilleures mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [2][1]).

Le document *Conseils sur le renforcement de la sécurité de Microsoft Windows 10 Enterprise (ITSP.70.012)* traite des outils et des fonctions de sécurité de Microsoft qu'il est possible d'utiliser pour renforcer la sécurité des systèmes d'exploitation Windows 10 Enterprise (« Windows 10 »). Il fait mention de certaines solutions de contournement et de certains correctifs apportés à des problèmes de sécurité connus dans Windows 10 (version 1607). Bien que le présent document ait été essentiellement rédigé à l'intention des ministères du gouvernement du Canada (GC), les organismes qui ne font pas partie du GC peuvent également mettre en pratique ces recommandations. Ces recommandations ne concernent que les points terminaux fonctionnant sous Windows 10, et non ceux sous Windows Server.

Ce document introduit les deux configurations de référence associées aux paramètres des objets de stratégies de groupe (GPO pour *Group Policy Object*). Ces deux configurations de référence comprennent des paramètres de références minimales et avancées. Les paramètres de références principales correspondent aux normes minimales requises pour les ministères du GC. Ils permettent d'assurer le même niveau d'atténuation contre les menaces à la sécurité à la plupart des points terminaux. Si les systèmes et réseaux contiennent de l'information Protégé B, il est impératif de mettre en œuvre les paramètres de références avancées, ainsi que des mesures de sécurité additionnelles qui sortent de la portée du présent document.

Ce document seulement présente les configurations de référence. Consultez les instructions pour obtenir une copie de la référence de sécurité du GC pour Windows 10 [1] à la section 8.1 de ce document.

Le CCC collabore avec Services partagés Canada (SPC) à l'élaboration de ces paramètres de GPO afin de limiter le risque qu'un auteur de menace compromette les biens de TI du GC contenus dans les outils informatiques communs, de même que dans les systèmes et les réseaux connectés à Internet. La compromission des systèmes et des réseaux entraîne des coûts importants et constitue une menace à la disponibilité, à la confidentialité et à l'intégrité des ressources d'information. Les ministères du GC doivent mettre en œuvre les paramètres de référence de manière à uniformiser la configuration des ordinateurs de bureau. Le recours à des bureaux standards permet de réaliser d'importantes économies sur le plan de la sécurité et de simplifier la gestion des correctifs personnalisés.

1.1 FACTEURS POLITIQUES

Les ministères du GC doivent se conformer aux exigences qui sont établies dans les politiques du Secrétariat du Conseil du Trésor (SCT) suivantes :

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

- Politique sur la gestion des technologies de l'information [3]
- Politique sur la sécurité du gouvernement [4]
- Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information [5]
- Directive sur la migration et la configuration du système d'exploitation de bureau Windows 10 : Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI) [6]

Il pourrait être utile pour les organismes qui ne font pas partie du GC de consulter ces politiques au moment d'élaborer leur cadre stratégique.

1.2 ENVIRONNEMENTS CONCERNÉS

L'orientation fournie par le présent document ne vise que les systèmes de TI non classifiés susceptibles de contenir de l'information ou des biens sensibles qui peuvent raisonnablement causer préjudice à un intérêt individuel, comme une personne ou un organisme (c.-à-d. l'information personnelle[2] et l'information opérationnelle[3]). Dans le contexte du GC, cette orientation peut viser les systèmes de TI qui contiennent de l'information Protégé A et/ou Protégé B.

Le présent document n'offre aucune orientation pour ce qui est des systèmes de TI qui contiennent de **l'information ou des biens hautement sensibles d'un intérêt individuel** (p. ex. l'information Protégé C dans le contexte du GC) et **l'information ou les biens sensibles d'un intérêt national** (p. ex. l'information classifiée[4]). Les systèmes de TI qui contiennent ce type d'information peuvent faire l'objet d'autres considérations de conception qui sortent de la portée du présent document.[5]

1.3 RELATION AVEC LE PROCESSUS DE GESTION DES RISQUES LIÉS AUX TI

Les ministères devraient tenir compte des paramètres de référence mentionnés dans le présent document au moment de planifier et de réaliser la mise en œuvre Windows 10. Il leur incombe d'établir des exigences et d'élaborer un cadre de gestion des risques qui permettra d'assurer une protection adéquate de l'information et des services.

L'*ITSG-33 La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie* [6] décrit deux niveaux d'activités de gestion des risques liés à la sécurité des TI, à savoir les activités du niveau ministériel et du niveau des systèmes d'information. La figure 1 à la page suivante donne un aperçu de ces activités.

---

[2] Tel qu'il est défini dans la Loi sur la protection des renseignements personnels et la Loi sur la protection des renseignements personnels et les documents électroniques, on entend, par renseignements personnels, tous les renseignements concernant un individu identifiable qui sont sauvegardés sous une forme quelconque.

[3] Dans ce contexte, on entend, par information opérationnelle, l'information qui peut raisonnablement causer préjudice à un organisme, conformément à ce qui est stipulé au paragraphe 20(1) de la Loi sur l'accès à l'information.

[4] Dans le contexte du GC, on entend, par information classifiée, toute information ou tout bien dont on peut raisonnablement s'attendre, lorsqu'ils sont compromis, à ce qu'ils causent un préjudice à l'intérêt national, à la défense et au maintien de la stabilité sociopolitique et économique du Canada. L'information est classifiée au niveau Confidentiel, Secret et Très secret, selon son type et le préjudice potentiel.

[5] Pour obtenir des conseils en matière de TI pour les environnements PROTÉGÉ C ou classifiés, prière de communiquer avec le Centre d'appels.

1.3.1 ACTIVITÉS DE NIVEAU MINISTÉRIEL

Au niveau du ministère, les activités sont intégrées au programme de sécurité du ministère pour planifier, gérer, évaluer et améliorer la gestion des risques à la sécurité des TI. Ces activités sont décrites en détail à l'annexe 1 de l'ITSG-33 [7].

1.3.2 ACTIVITÉS DU NIVEAU DU SYSTÈME D'INFORMATION

Les activités visant l'ensemble du système d'information sont intégrées au cycle de vie de l'information. Elles sont menées pour veiller à :

- répondre aux besoins opérationnels en matière de sécurité des TI
- mettre en œuvre les contrôles de sécurité appropriés et les exploiter comme prévu
- réaliser l'évaluation des performances des contrôles de sécurité mis en œuvre et faire rapport des résultats pour veiller à ce que les problèmes soient abordés

L'annexe 2 de l'ITSG-33 [8] décrit les activités de gestion des risques liés à la sécurité des TI nécessaires à la mise en œuvre, à l'exploitation et au maintien de systèmes d'information fiables tout au long de leur cycle de vie. L'annexe 2 du guide [8] propose également un processus de cycle de développement des systèmes (CDS) sécurisé appelé processus d'application de la sécurité dans les systèmes d'information (PASSI).

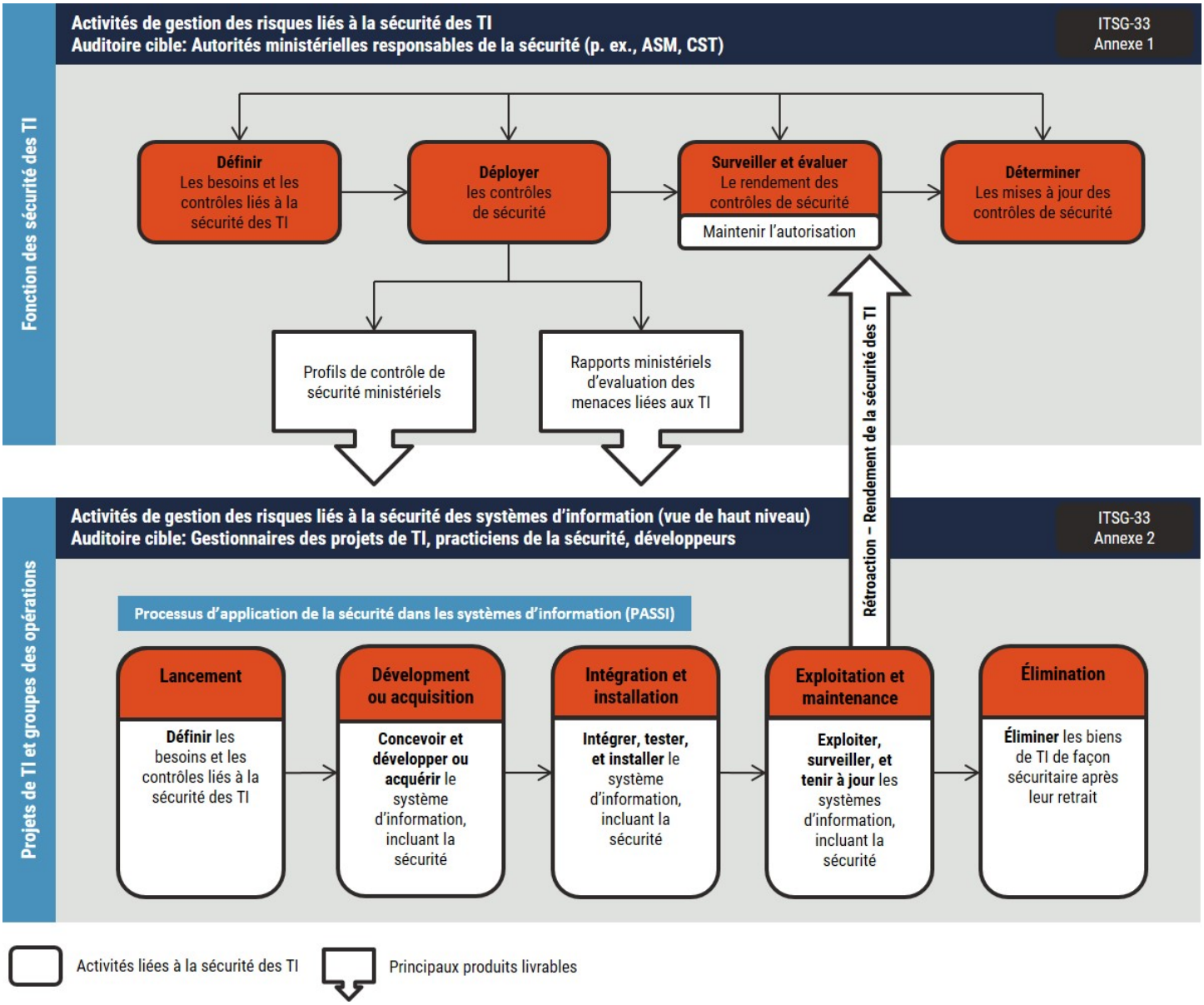

Figure 1: Activités de gestion des risques liés à la sécurité des TI

2 POINTS À CONSIDÉRER

Avant de reconfigurer ou de mettre à niveau les systèmes de TI ou leurs composants, les ministères devraient tenir compte des exigences de sécurité et des besoins opérationnels qui leur sont propres en faisant ce qui suit :

- définir toutes les exigences liées à la sécurité et la conception de l'architecture d'entreprise
- réaliser une évaluation des menaces et des risques (EMR)
- déterminer les composants matériels et micrologiciels des points terminaux

2.1 EXIGENCES LIÉES À LA SÉCURITÉ ET LA CONCEPTION DE L'ARCHITECTURE D'ENTREPRISE

Toutes les exigences liées à la sécurité et la conception de l'architecture d'entreprise doivent être définies avant d'appliquer les recommandations formulées dans le présent document. Une image complète de l'architecture d'entreprise permettra aux ministères de déterminer les outils et les fonctions de sécurité qui conviennent à leurs besoins opérationnels et à leurs exigences en matière de sécurité. Les ministères devraient continuer de surveiller les outils et les fonctions de sécurité après leur mise en œuvre dans le cadre des activités permanentes de gestion des risques. Une surveillance régulière permettra ainsi d'assurer l'efficacité des contrôles de sécurité.

2.2 ÉVALUATIONS DES MENACES ET DES RISQUES

Les ministères devraient mener une évaluation des menaces et des risques (EMR) dans le cadre de leurs activités de gestion des risques. Une EMR devrait définir les besoins opérationnels et en matière de sécurité, ainsi qu'indiquer la posture de sécurité actuelle du ministère et inclure tous les contrôles de sécurité prévus ou existants. Les ministères peuvent utiliser les résultats de leurs EMR pour déterminer la configuration de Windows 10 qui convient le mieux à leurs besoins. S'ils ne sont pas en mesure de procéder à une mise à niveau ou à une reconfiguration immédiate de Windows 10, les ministères devraient déterminer les stratégies et les mesures de sécurité provisoires à mettre en place d'après les résultats de leurs EMR.

2.3 MATÉRIEL ET MICROLOGICIELS

Les ministères devraient prendre en considération le matériel et les micrologiciels au moment de procéder à l'achat et à la mise en œuvre des points terminaux (p. ex. serveurs, ordinateurs de bureau, ordinateurs portatifs, tablettes). Les nouveaux points terminaux devraient être configurés au moyen des composants matériels et micrologiciels mentionnés dans les lignes directrices de Microsoft sur la sécurité des appareils [8].[6] Pour tirer parti des nouvelles fonctions de sécurité de Windows 10, les composants matériels et micrologiciels suivants devraient être mis en place :

[6] Les lignes directrices de Microsoft sur la sécurité des appareils sont en voie de devenir la norme dans l'industrie.

- l'interface micrologicielle extensible unifiée (UEFI pour *Unified Extensible Firmware Interface*) (non configurée pour être exécutée en mode de système d'entrée-sortie de base [BIOS pour *Basic Input/Output System*] patrimonial) pour permettre le démarrage sécurisé. L'UEFI doit prendre en charge les mises à jour micrologicielles sécurisées.
- le module de plateforme sécurisée 2.0 (TPM pour *Trusted Platform Module*). Certains dispositifs utilisant le module TPM 1.2 peuvent être mis à niveau.
- le formatage du disque dur avec la table de partition d'identificateur global unique (GUID pour *Global Unique Identifier*) (et non l'enregistrement de démarrage principal [MBR pour *Master Boot Record*]).
- l'intégrité du code protégé par hyperviseur (HVCI pour *Hypervisor Code Integrity*) pour assurer la mise en œuvre de Device Guard.
- une unité centrale de traitement (UCT) de 64 bits avec la technologie de virtualisation Intel (VT-x) ou Advanced Micro Dynamics (AMD-V), et les tables de pages étendues, aussi appelées traduction d'adresse de second niveau (SLAT pour *Second Level Address Translation*).

3 STRATÉGIE D'ATTÉNUATION

Pour prévenir les compromissions d'actifs et d'infrastructures connectés à Internet, dix mesures de sécurité ont été recommandées dans *l'ITSM.10.189 – Les 10 meilleures mesures de sécurité des TI visant à protéger les réseaux Internet et l'information* [1]. L'une de ces mesures de sécurité consiste à renforcer la sécurité des systèmes d'exploitation en désactivant tous les ports et les services non essentiels, en supprimant les comptes inutiles, en évaluant les applications de tierces parties et en appliquant des contrôles de sécurité plus poussés. Lorsqu'il s'agit de déterminer la façon de renforcer la sécurité des systèmes d'exploitation, l'utilisation de la configuration par défaut (originale) de Windows 10 ne fournit pas le niveau de sécurité adéquat pour les systèmes de TI, les réseaux et les ressources d'information du GC. Il est donc recommandé de configurer Windows 10 avec les fonctions de sécurité mentionnées à la section 4.1 du présent document.

En ce qui concerne les paramètres de GPO, les ministères sont tenus de mettre en place les paramètres de références minimales décrits à la section 5 du présent document. Les paramètres de références minimales représentent la norme de sécurité minimale pour les ministères du GC, puisqu'ils permettent d'assurer le même niveau d'atténuation contre les menaces à la sécurité à la plupart des points terminaux. Les ministères au sein desquels on retrouve des systèmes de TI non classifiés susceptibles de contenir de l'information ou des biens sensibles qui peuvent raisonnablement causer préjudice à un intérêt individuel (p. ex. une personne ou un organisme) exigent des niveaux de sécurité additionnels. Dans le contexte du GC, cette catégorie d'information correspond à de l'information Protégé B. Afin d'assurer une meilleure protection de l'information sensible, les ministères au sein desquels on retrouve des systèmes fonctionnant dans des environnements Protégé B doivent mettre en place les paramètres de références avancées, ainsi que des mesures additionnelles qui ne sont pas abordées dans le présent document.

> **Nota :** Selon les résultats de l'EMR, les ministères pourraient conclure qu'il est préférable de mettre en place une fonction de sécurité additionnelle pour protéger les opérations Protégé B.

Pour renforcer la sécurité des systèmes d'exploitation, il est recommandé à tous les ministères de mettre en place les paramètres de références minimales et avancées. Ces paramètres devraient être mis en œuvre avec des mesures de sécurité additionnelles pour répondre aux besoins propres au ministère.

4 CONFIGURATION DE WINDOWS 10

Le renforcement de la sécurité des systèmes d'exploitation n'est qu'une des 10 meilleures mesures de sécurité des TI recommandées par le CCC. Il est possible de renforcer la sécurité des systèmes d'exploitation en ajoutant des fonctions de sécurité à leur configuration. Cette section décrit les outils et les fonctions de sécurité de Windows 10 qu'il est recommandé de mettre en œuvre [5].

4.1 OUTILS ET FONCTIONS DE SÉCURITÉ RECOMMANDÉS DE WINDOWS

Windows 10 devrait être configuré avec les fonctions de sécurité et les améliorations mentionnées dans le tableau 1. Toutes ces fonctions de sécurité et améliorations sont soit comprises dans Windows 10 (version 1607), soit offertes gratuitement par Microsoft.

Tableau 1. Fonctions de sécurité et améliorations recommandées de Windows 10

Fonction	Description
BitLocker	Fonction de chiffrement intégral du disque dur validée par le Programme de validation des modules cryptographiques (PVMC). Elle permet de protéger les données inactives dans l'environnement de Windows 10 contre les attaques hors ligne ou les démarrages malveillants à partir d'un autre système d'exploitation. Au moment de chiffrer les données du GC, il est primordial de configurer BitLocker conformément aux normes du Federal Information Processing Standards (FIPS). **Nota** : Il n'est pas recommandé d'utiliser des modules PVMC ne fonctionnant pas en mode FIPS pour chiffrer l'information du GC.
Enhanced Mitigation Experience Toolkit (EMET)	Utilitaire permettant d'éviter l'exploitation des vulnérabilités présentes dans les logiciels inclus dans les applications traditionnelles et tierces. Les techniques d'atténuation des risques employées par l'utilitaire EMET comprennent notamment la prévention de l'exécution des données, la protection structurée contre le remplacement du gestionnaire d'exceptions et la programmation orientée anti-retour. **Nota** : L'utilitaire EMET est désuet et ne sera plus pris en charge dans la mise à jour *Windows 10 Fall Creators Update (1709)* [10]. Il a été déployé dans la fonctionnalité Exploit Protection de Windows Defender Exploit Guard.
AppLocker	Complément à la politique de restriction liée aux logiciels précédemment mise en place par Microsoft. Il propose des options de définition souples pour l'établissement de listes blanches. Les technologies de liste blanche d'applications contrôlent les applications qui peuvent être installées ou exécutées sur un hôte. L'établissement de listes blanches est l'une des principales mesures recommandées dans l'ITSM.10.189 [1]. Pour de plus amples renseignements, voir l'*ITSB-95 – Utilisation d'une liste blanche des applications* [11].
Démarrage sécurisé	Norme de sécurité utilisée pour vérifier que les points terminaux démarrent uniquement à l'aide d'un logiciel approuvé par le fabricant du PC. Chaque composante du logiciel est validée à partir d'une base de données contenant les signatures saines connues qui sont maintenues dans le micrologiciel.

Fonction	Description
Device Guard	Ensemble de fonctionnalités matérielles et de sécurité qui utilise la sécurité basée sur la virtualisation pour veiller à ce que le système d'exploitation exécute uniquement les applications de confiance mentionnées dans les stratégies d'intégrité du code du ministère.
Credential Guard	Fonctionnalité de Windows 10 qui permet de protéger les systèmes contre les attaques par vol de justificatifs d'identité. La fonctionnalité Credential Guard utilise la sécurité basée sur la virtualisation pour isoler les secrets (p. ex. les condensés de mots de passe du protocole d'identification NTLM [New Technology Local Area Network Manager] et les tickets TGT [Ticket Granting Ticket] de Kerberos) du reste du système d'exploitation.
Microsoft Desired Configuration Manager (DCM)	Fonction de l'outil Security Compliance Manager (SCM) de Microsoft qui permet d'évaluer la conformité d'un hôte Windows en fonction des exigences minimales désirées. La vérification de la conformité comprend notamment la version du système d'exploitation, la configuration des applications, les mises à jour et d'autres paramètres de sécurité. **Nota** : Le nouveau nom de cette fonctionnalité est « Paramètres de compatibilité » dans la branche actuelle de System Center Configuration Manager [12]. Les paramètres de conformité permettent d'effectuer ce qui suit : • Comparer la configuration des PC Windows, des ordinateurs Mac, des serveurs et des dispositifs mobiles, et les gérer conformément aux configurations qui ont été créées ou obtenues d'autres fournisseurs. • Déceler les configurations de dispositifs non autorisées. • Faire rapport de la conformité aux politiques réglementaires et aux politiques de sécurité internes. • Cerner les vulnérabilités de sécurité. • Fournir au service de dépannage l'information nécessaire pour détecter les causes probables des incidents et des problèmes signalés par l'identification des configurations non conformes. • Corriger automatiquement certains paramètres non conformes sur les dispositifs mobiles. Les paramètres de conformité permettent également de cerner les vulnérabilités de « non-conformité » et d'y remédier en journalisant la « non-conformité » des applications, des paquets et programmes, ou des scripts dans un magasin de fichiers communs. La « non-conformité » des dispositifs est régulièrement enregistrée dans le magasin de fichiers communs.
Environnement isolé de conversion Microsoft Office (MOICE pour *Microsoft Office Isolated Conversion Environment*)	Fonctionnalité nouvellement ajoutée au Module de compatibilité Microsoft Office qui permet d'ouvrir en toute sécurité les fichiers binaires de Word, Excel et PowerPoint enregistrés dans les courriels sous forme de pièce jointe. **Nota** : MOICE est une fonctionnalité d'Office 2007 qui a été déployée dans le mode protégé[7] d'Office 2010 et des versions subséquentes.

[7] Le mode protégé est une nouvelle fonction de sécurité d'Office 2013 qui a été tirée de l'environnement isolé de conversion Microsoft Office (MOICE) dans Office 2007. Il aide à atténuer les risques d'exploitation de l'ordinateur en ouvrant les fichiers dans un environnement restreint à des fins d'examen avant qu'ils ne soit ouverts pour modification dans Microsoft Excel 2013, PowerPoint 2013 ou Word 2013. Le mode protégé ouvre les fichiers potentiellement dangereux dans un environnement de type bac à sable. (Microsoft. *What is Protected View?* [12])

4.2 CONSÉQUENCES DU DÉPLOIEMENT DE LA CONFIGURATION PAR DÉFAUT

Les ministères peuvent aider à renforcer la sécurité de leurs systèmes d'exploitation en déployant Windows 10 avec des configurations mises à jour, tirant ainsi parti de la gamme complète de fonctions de sécurité mentionnées dans le tableau 1 ci-dessus. Du point de vue de la sécurité, la configuration par défaut (originale) de Windows 10 ne respecte pas le niveau de sécurité exigé pour les ministères du GC. Si ces derniers ont recours à la configuration par défaut, il est fortement recommandé de mettre en œuvre les fonctions de sécurité et les paramètres de référence [1].

5 PARAMÈTRES DE GPO

En collaboration avec SPC, le CCC a établi les bases des paramètres de GPO dans Windows 10 (version 1607).
Ces paramètres appartiennent à deux catégories : les paramètres de références principales minimales et les paramètres de références avancées additionnels. Prière de communiquer avec le Centre d'appels du CCC pour obtenir copie de l'annexe A [2], qui présente une liste des paramètres pour ces deux configurations de référence.

Pour établir ces paramètres, l'organisme a consulté les publications d'orientation en matière de configuration élaborées par d'autres organismes :

- Center for Internet Security (CIS) – *Securing Microsoft Windows Desktop* [14]
- Defense Information Systems Agency (DISA) – *Windows 10 Security Technical Implementation Guide* (STIG) [15]
- Microsoft Security Guidance Blog – *Security Baseline for Windows 10 v1607 ("Anniversary Edition") and Windows Server 2016* [16]

5.1 PARAMÈTRES DE RÉFÉRENCES MINIMALES

Les paramètres de références minimales représentent la norme de sécurité minimale pour les ministères du GC. Ils sont obligatoires pour les ministères du GC, puisqu'ils permettent d'assurer à la plupart des points terminaux le même niveau de sécurité requis pour protéger les ressources d'information et l'infrastructure du GC contre les menaces.

Ces paramètres figurent à dans les configurations de référence de sécurité pour Windows 10 [1] sous la désignation « Référence minimales ». Certains paramètres ont été sélectionnés en vue de les incorporer au programme. Bien qu'il soit possible d'obtenir les mêmes résultats en laissant ces paramètres « non configurés », la sélection du paramètre est davantage conforme à la version de référence et permet de contrôler les mises à jour automatiques ou recommandées à venir qu'il pourrait être nécessaire de passer en revue avant leur mise en œuvre.

5.2 PARAMÈTRES DE RÉFÉRENCES AVANCÉES

Les paramètres de références avancées correspondent aux paramètres du système d'exploitation qui permettent de prendre en charge les environnements Protégé B. Les paramètres de références avancées, ainsi que les mesures additionnelles qui ne sont pas abordées dans le présent document, doivent être mis en place afin d'assurer une plus grande protection de l'information sensible. Ils figurent dans les configurations de référence de sécurité pour Windows 10 [1] sous la désignation « Référence avancée ».

6 MISE EN ŒUVRES DES GPO – SOLUTIONS DE CONTOURNEMENT ET CORRECTIFS

Plusieurs solutions de contournement et correctifs propres à la version 1607 sont mentionnés un peu plus loin dans ce document.

6.1 MODE FIPS

Recommandation : activer le mode FIPS.

Le mode FIPS devrait être activé et utilisé dans Windows 10. Seuls les algorithmes approuvés par le CCC (et, par le fait même, approuvés selon FIPS) devraient être utilisés pour protéger l'information sensible.

Les algorithmes sont inhérents à la fonctionnalité du mode FIPS.

Les applications doivent faire l'objet de tests en vue de déterminer si Windows 10 peut fonctionner correctement en mode FIPS dans un environnement donné. Advenant le moindre problème ou la moindre inquiétude, prière de communiquer avec le Centre d'appels du CCC pour obtenir de l'assistance.

6.2 PAIR À PAIR

Recommandation : les services réseau pair à pair ne devraient pas être configurés (c.-à-d. utiliser le paramètre par défaut).

Le paramètre de GPO « Désactiver les services réseau pair à pair Microsoft » a été mis en place dans Windows XP. Il permettait de verrouiller des fonctionnalités spécifiques, comme les communications en temps réel (p. ex. la messagerie instantanée sans serveur, le jumelage en temps réel et la jouabilité), l'Espace de collaboration Windows, la distribution de contenu et le traitement distribué. Pour de plus amples renseignements, voir le document Introduction to *Windows Peer-to-Peer Networking* [17].

Les technologies pair à pair modernes qui ont vu le jour après Windows XP, telles que Windows BranchCache (mode pair à pair), le cache d'homologue pour ConfigMgr (version 1610 et ultérieures) et l'optimisation de la distribution de Windows Updates, sont essentielles au déploiement efficace et au maintien du cycle de vie (c. à d. l'application de correctifs, l'installation de logiciels et les Services de maintenance Windows) des ordinateurs de bureau fonctionnant sous Windows 10. Ces technologies pair à pair permettent d'éviter le recours à de l'équipement réseau coûteux à chaque emplacement avec une bande passante sous-optimale.

L'activation de ce paramètre ne devrait avoir aucune incidence. Il s'applique au regroupement du protocole PNRP (Peer Name Resolution Protocol) patrimonial, ainsi qu'aux protocoles PPGRH (Peer-to-Peer Graphing) et PNM (People Near Me), qui sont toujours utilisés dans le Groupement résidentiel. Par exemple :

- L'optimisation de la distribution de Windows Updates (WUDO pour *Windows Updates Delivery Optimization*) et BranchCache ne sont pas visés, puisqu'ils sont conçus à partir d'autres composants.
- Le cache d'homologue pour ConfigMgr n'est pas visé, puisque la découverte des caches d'homologue est gérée par les points de gestion de ConfigMgr, et la diffusion de contenu est effectuée au moyen du protocole de transfert hypertexte (HTTP pour HyperText Transfer Protocol) et du protocole de transfert hypertexte sécurisé (HTTPS pour *HyperText Transfer Protocol Secure*).

6.3 POWERSHELL

On ne peut désactiver PowerShell[8] , puisqu'il s'agit d'un composant essentiel du système d'exploitation et de plusieurs applications. Il existe toutefois différents moyens d'ajouter des restrictions pour les utilisateurs sans privilèges. Il importe de tenir compte de ce qui suit :

- Un script PowerShell ne s'exécutera qu'avec les mêmes autorisations que l'utilisateur ou le processus utilisé pour lancer le script.
- Windows 10 est livré avec PowerShell 5.0, une version plus sécurisée de PowerShell qui offre un plus grand nombre de fonctions de journalisation et de détection que les versions précédentes. Ces fonctions sont décrites dans le document *Advances in Scripting Security and Protection in Windows 10 and PowerShell V5* [17].
- PowerShell est assujettie à plusieurs niveaux de stratégies d'exécution qu'il est possible de définir au moyen d'un GPO, tel qu'il est indiqué dans le document *About Execution Policies* [18] (voir le tableau 2 pour une description des niveaux des stratégies d'exécution).
- Les dispositifs devraient être configurés au niveau **Restricted** ou **AllSigned** pour assurer une sécurité et une polyvalence maximum.

Tableau 2. Niveaux des stratégies d'exécution de PowerShell

Niveau de stratégie d'exécution	Description
Niveau Restricted	• Stratégie d'exécution par défaut de Windows 8, Windows Server 2012 et Windows 8.1. • Autorise les commandes individuelles, mais n'exécute aucun script. • Prévient l'exécution de tous les fichiers de script, notamment les fichiers de formatage et de configuration (.ps1xml), les fichiers de script du module (.psm1) et les profils Windows PowerShell (.ps1).

[8] PowerShell est le shell de commande actuel pour Windows. Depuis la publication 1511 de Windows 10, PowerShell est le shell de commande par défaut, qui remplace l'invite de commande de Windows NT (CMD.EXE).

Niveau de stratégie d'exécution	Description
Niveau AllSigned	• L'exécution des scripts est autorisée. • Exige que tous les scripts et les fichiers de configuration soient signés par un éditeur approuvé, ce qui comprend les scripts que l'utilisateur écrit sur l'ordinateur local. • Invite l'utilisateur à confirmer l'exécution des scripts provenant d'éditeurs n'ayant pas encore été approuvés ou interdits. • Risques d'exécution de scripts signés, mais malveillants.
Niveau RemoteSigned	• L'exécution des scripts est autorisée. Il s'agit de la stratégie d'exécution par défaut de Windows Server 2012 R2. • Exige la signature numérique d'un éditeur approuvé avant que des scripts et des fichiers de configuration ne soient téléchargés depuis Internet (ce qui comprend les programmes de messagerie électronique et de messagerie instantanée). • N'exige aucune signature numérique pour les scripts qui ont été écrits par l'utilisateur sur l'ordinateur local (non téléchargés depuis Internet). • Exécute les scripts téléchargés depuis Internet et ceux qui ne sont pas signés si les scripts en question sont débloqués (p. ex. au moyen de l'applet de commande Unblock-File). • Risques d'exécution de scripts non signés de sources autres qu'Internet et de scripts signés, mais malveillants.
Niveau Unrestricted	• L'exécution des scripts non signés est autorisée. Risque d'exécution de scripts malveillants. • L'utilisateur est avisé avant l'exécution des scripts et le téléchargement des fichiers de configuration depuis Internet.
Niveau Bypass	• Rien n'est bloqué. Aucun avertissement et aucune invite. • Cette stratégie d'exécution vise les configurations dans lesquelles 1) un script Windows PowerShell est intégré dans une application plus grande ou 2) Windows PowerShell est à la base d'un programme qui emploie son propre modèle de sécurité.

6.4 MODE DE VEILLE DES TABLETTES

Recommandation : utiliser les paramètres du mode veille mentionnés dans le tableau 3.

Tableau 3. Paramètres du mode veille recommandés

Paramètre	Référence minimale	Référence avancée
Autoriser les états de veille (S1-S3) lorsque l'ordinateur est en veille (sur batterie)	Désactivé	Activé
Autoriser les états de veille (S1-S3) lorsque l'ordinateur est en veille (sur secteur)	Désactivé	Activé
Spécifier le délai de veille prolongée du système (sur batterie)	Non configuré	Activé
Spécifier le délai de veille prolongée du système (sur secteur)	Non configuré	Activé

Windows 10 prend en charge plusieurs états de veille sur des dispositifs compatibles, tel qu'il est indiqué dans le document System Sleeping States [20]. Les quatre états communément utilisés sur le matériel moderne sont les suivants :

- S0 (système en fonction)
- S3 (veille)
- S4 (veille prolongée)
- S5 (arrêt du système)

> **Remarque :** Les états S1 et S2 ne sont pas mentionnés dans le tableau ci-dessous, puisqu'ils ne sont pas touchés par les problèmes mentionnés. Pour de plus amples renseignements sur les états S1 et S2, prière de consulter le document *System Sleeping States* [20].

Si un dispositif est chiffré avec BitLocker en faisant appel à la protection du module de TPM et à un numéro d'identification personnel (NIP), seuls les dispositifs dont le démarrage s'effectue depuis un état de mise hors tension (S4 ou S5) exigeront la saisie d'un NIP. Les systèmes qui sortent du mode veille depuis d'autres états de veille, comme le mode S3, passeront directement à l'écran de verrouillage sans exiger la saisie d'un NIP.

On utilise le paramètre de stratégie de groupe « \Système\Gestion de l'alimentation\Paramètres de la veille\Demander un mot de passe lorsqu'un ordinateur sort de la veille » pour obliger l'utilisateur à s'authentifier de nouveau au moment de reprendre une session utilisateur.

Tableau 4. Modes veille des tablettes

État de veille	Configuration et caractéristiques
Mode actif du système S0	**Consommation électrique** Maximale. Il est toutefois possible de modifier l'état d'alimentation des dispositifs individuels de façon dynamique, puisque l'économie d'énergie est réalisée sur chacun des dispositifs. Les dispositifs non utilisés peuvent être mis sous et hors tension au besoin. **Reprise logicielle** Sans objet. **Latence matérielle** Aucune. **Contexte matériel du système** Tout le contexte est conservé.
État de l'alimentation système S3	**Consommation électrique** Inférieure à la consommation à l'état S2. Le processeur est éteint et

État de veille	Configuration et caractéristiques
	certaines puces de la carte mère pourraient être éteintes. **Reprise logicielle** Après la mise en éveil, le contrôle démarre à partir du vecteur de réinitialisation du processeur. **Latence matérielle** Quasi indifférentiable de l'état S2. **Contexte matériel du système** Seule la mémoire système est conservée. Le contexte de l'UCT, le contenu des caches et le contexte des jeux de puces sont perdus.
État de l'alimentation système S4 L'état de l'alimentation système S4 – l'état de veille prolongée – est l'état de veille qui consomme le moins d'énergie et offre la plus longue latence à la sortie de veille. Pour réduire la consommation d'énergie au minimum, le matériel met hors tension tous les dispositifs. Le contexte du système d'exploitation est conservé dans un fichier de mise en veille prolongée (une image mise en mémoire) que le système écrit sur le disque avant de passer à l'état S4. Au redémarrage, le chargeur lit ce fichier et accède à l'emplacement de préparation de mise en veille prolongée précédemment utilisé par le système. Si un ordinateur à l'état S1, S2 ou S3 n'est pas alimenté par le secteur ou la batterie, son contexte matériel est perdu et il doit être redémarré pour revenir à l'état S0. Un ordinateur à l'état S4 peut être redémarré depuis son emplacement précédent, même s'il n'est pas alimenté par le secteur ou la batterie, puisque le contexte du système d'exploitation est conservé dans le fichier de mise en veille prolongée. Un ordinateur à l'état de veille prolongée ne consomme aucune énergie (à l'exception, peut-être, du courant de soutien).	**Consommation électrique** Désactivée, à l'exception du courant de soutien du bouton d'alimentation et des dispositifs similaires. **Reprise logicielle** Le système redémarre à partir du fichier de mise en veille prolongée. Un redémarrage est nécessaire s'il est impossible de charger le fichier de mise en veille prolongée. Reconfigurer le matériel alors que le système est à l'état S4 risque d'entraîner des changements susceptibles de nuire au chargement du fichier de mise en veille prolongée. **Latence matérielle** Longue et non définie. La moindre interaction physique fait passer le système au mode actif. Une interaction peut prendre les formes suivantes : un utilisateur qui appuie sur le bouton de mise en marche ou encore, si le système est doté du matériel approprié et si la mise en éveil est activée, un appel entrant reçu par le modem ou une activité sur un réseau local. Un système peut également être mis en éveil à la reprise d'un minuteur, si le matériel le prend en charge. **Contexte matériel du système** Rien n'est conservé dans le matériel. Le système crée une image de la mémoire dans le fichier de mise en veille prolongée avant de s'éteindre. Lors de son chargement, le système d'exploitation lit ce fichier et accède à l'emplacement précédemment utilisé.
État d'arrêt de système S5 À l'état S5, ou à l'état d'arrêt, aucune mémoire n'est chargée dans la machine et aucun calcul n'est effectué. On établit qu'une seule distinction entre les états S4 et S5. À l'état S4, l'ordinateur peut redémarrer depuis le fichier de mise en veille prolongée, alors qu'à l'état S5, il est nécessaire de procéder au réamorçage du système.	**Consommation électrique** Désactivée, à l'exception du courant d'entretien des dispositifs comme le bouton de mise en marche. **Reprise logicielle** Redémarrage obligatoire à la mise en éveil. **Latence matérielle** Longue et non définie. La moindre interaction physique, comme l'utilisateur qui appuie sur le bouton de mise en marche, fait passer le système au mode actif. Le BIOS peut également être mis en éveil à la reprise d'un minuteur, si le système est ainsi configuré. **Contexte matériel du système** Rien n'est conservé.

7 ÉVOLUTION CONTINUE, VERSIONS ET CONTRÔLE DE VERSIONS

Le présent document fait mention des éléments de référence fondamentaux qui permettront de renforcer la sécurité des systèmes d'exploitation de Windows 10. Le présent document décrit les paramètres de GPO et les opérations que l'on retrouve dans la version 1607 de Windows 10.

Les outils et les fonctions de sécurité mentionnés constituent les plus récents services offerts par Microsoft pour Windows 10 (version 1607) au moment de publier le présent document. Microsoft a annoncé que des améliorations continues seraient apportées à Windows 10. De nouvelles versions devraient donc être diffusées tous les six mois. Ce document pourrait être mis à jour afin de faire mention de l'ensemble des outils et des fonctions de sécurité pertinents. Les changements majeurs ou les ajouts visant les solutions de contournement et les correctifs décrits dans le présent document seront diffusés sous forme d'addenda.

8 RÉSUMÉ

Windows 10 offre des outils et des fonctions de sécurité à jour qui devraient être utilisés pour développer des outils informatiques communs sécurisés pour les ministères du GC. Pour obtenir une copie des paramètres détaillés des GPO, voir la section 8.1 ci-dessous. Le CCC a collaboré avec SPC et les responsables de Microsoft Canada à l'établissement de ces paramètres. Les paramètres de références minimales et avancées sont conformes aux exigences du GC en matière de sécurité des TI.

Bien que ces références soient une composante obligatoire de la mise en place d'une posture de sécurité commune à tous les points terminaux du GC, certaines variantes ou modifications pourraient être requises pour répondre aux exigences de sécurité et aux besoins opérationnels des ministères, qui ont été relevés dans les EMR. Toutes les exigences qui en ont découlé doivent être adéquatement documentées.

8.1 AIDE ET RENSEIGNEMENTS

Pour de plus amples renseignements ou des conseils, prière de communiquer avec les Services à la clientèle de la STI.

Centre d'appels

contact@cyber.gc.ca

613-949-7048 ou 1-833-CYBER-88

Pour obtenir une copie de la dernière version des configurations de référence de sécurité pour Windows [1], envoyer un courriel à SPC à l'adresse suivante :

SSC.DesktopOSImaging-ImagedesSOdetravail.SPC@canada.ca

Les ministères du GC peuvent également en obtenir un exemplaire via GCconnex. Inscrivez-vous au groupe GCconnex de « WTD Common Desktop Operating Environment – Environnement d'exploitation commun des ordinateurs de bureau des ATMT ».

9 CONTENU COMPLÉMENTAIRE

9.1 LISTE D'ABRÉVIATIONS, D'ACRONYMES, ET DE SIGLES

Terme	Définition
AMD-V	Technologie de virtualisation AMD (Advanced Micro Dynamics Virtualization)
BIOS	Système d'entrée-sortie de base (Basic Input/Output System)
CCC	Centre canadien pour la cybersécurité
CDS	Cycle de développement des systèmes
CIS	Center For Internet Security
COMSEC	Sécurité des communications (Communications Security)
CST	Centre de la sécurité des télécommunications
DCM	Desired Configuration Manager
DISA	Defense Information Systems Agency
EMET	Enhanced Mitigation Experience Toolkit
EMR	Évaluation des menaces et des risques
FIPS	Federal Information Processing Standards
GC	Gouvernement du Canada
GPO	Objet de stratégie de groupe (Group Policy Object)
GUID	Identificateur global unique (Global Unique Identifier)
HTTP/HTTPS	Protocole HTTP/HTTPS (Hypertext Transfer Protocol/HTTP Secure)
HVCI	Intégrité du code protégé par l'hyperviseur (Hypervisor Code Integrity)
MBR	Secteur d'amorçage principal (Master Boot Record)
MOICE	Environnement isolé de conversion Microsoft Office (Microsoft Office Isolated Conversion Environment)
NIP	Numéro d'identification personnel
NTLM	Protocole d'identification NTLM (New Technology Local Area Network Manager)
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PNM	People Near Me
PNRP	Protocole PNRP (Peer Name Resolution Protocol)
PPGRH	Peer-to-Peer Graphing
PVMC	Programme de validation des modules cryptographiques
SCM	Security Compliance Manager
SCT	Secrétariat du Conseil du Trésor
SLAT	Traduction d'adresses de second niveau (Second Level Address Translation)

Terme	Définition
SPC	Services partagés Canada
STI	Sécurité des technologies de l'information
STIG	Security Technical Implementation Guide
TGT	Ticket Granting Ticket
TI	Technologies de l'information
TPM	Module de plateforme fiable (Trusted Platform Module)
UEFI	Interface micrologicielle extensible unifiée (Unified Extensible Firmware Interface)
VT-x	Technologie de virtualisation Intel
WUDO	Optimisation de la distribution de Windows Update (Windows Update Delivery Optimization)

9.2 RÉFÉRENCES

Numéro	Référence
1	Les configurations de référence de sécurité pour Windows du Services partagés Canada.
2	Centre de la sécurité des télécommunications. ITSM.10.189 Les 10 mesures de sécurité des TI visant à protéger les réseaux Internet et l'information. Octobre 2017.
3	Secrétariat du Conseil du Trésor du Canada. Politique sur la gestion des technologies de l'information. Juillet 2007.
4	Secrétariat du Conseil du Trésor du Canada. Politique sur la sécurité du gouvernement. Juillet 2009.
5	Secrétariat du Conseil du Trésor du Canada. Norme opérationnelle de sécurité : Gestion de la sécurité des technologies de l'information. Mai 2004.
6	Secrétariat du Conseil du Trésor du Canada. Avis de mise en œuvre de la Politique sur la technologie de l'information (AMPTI) Directive sur la migration et la configuration du système d'exploitation de bureau Windows 10. 10 août 2018.
7	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.
8	Microsoft. Device Security. 4 Mai 2017.
9	Microsoft. Features that are Removed or Deprecated in Windows 10 Fall Creators Update. 12 Décembre 2017.
10	Centre de la sécurité des télécommunications. ITSB-95 Utilisation d'une liste blanche des applications. Mars 2015.
11	Microsoft. Ensure Device Compliance with System Center Configuration Manager. 6 Octobre 2016.
12	Microsoft. What is Protected View? Sans date.
13	Center for Internet Security (CIS). Microsoft Windows Desktop CIS Benchmark. Sans date.
14	Defense Information Systems Agency (DISA). Windows 10 Security Technical Implementation Guide (STIG). 18 Août 2017.
15	Microsoft. Security Baseline for Windows 10 v1607. 17 Octobre 2016.
16	Microsoft. Introduction to Windows Peer-to-Peer Networking. 27 Septembre 2006.

Numéro	Référence
17	Microsoft. Advances in Scripting Security and Protection in Windows 10 and PowerShell V5. 10 Juin 2015.
18	Microsoft. About Execution Policies. Sans date.
19	Microsoft. System Sleeping States. 16 Juin 2017.