Titre :	**Exigences relatives à la sécurité des postes de travail corporatifs**		
État :	Approuvé	Effective à partir de :	2023-11-06
		Dernière mise à jour :	2023-11-06

Type :	Exigences		
Code du document :	MSSS-EXI-008	Portée :T	MSSS et RSSS
Mots clés :	BIOS, BitLocker ; Chiffrement ; Cryptage ; Démarrage système ; Logiciel malveillant ; Réduction surface d'attaque ; modules systèmes ; Correctif de sécurité ; Pare-feu système ; LAPS; compte administrateur local ; Logiciel malveillant ; LSA ; Périphériques amovibles; USB ; Menace Internet; menace Web ; Accès ; Verrouillage de cession.		
Justification :	Mesures offrant une protection minimale des postes de travail sous Windows.		

Déclaration :	**1. Mot de passe du BIOS (Basic Input Output System)**
Précisions :	
Le BIOS fournit un ensemble de services permettant de faire, en grande partie, abstraction de la couche matérielle. Ces services sont utilisés par le système d'exploitation essentiellement lors du processus de démarrage du poste de travail. L'accès aux paramètres du BIOS doit donc être protégé par un mot de passe afin de le protéger contre de possibles tentatives malveillantes visant notamment à altérer la séquence de démarrage et la désactivation des fonctions sécurisées.	
Justification :	• Limiter les actions de compromission en protégeant l'accès aux paramètres du BIOS. • Empêcher la modification de la séquence d'amorçage. • Garantir le démarrage du poste de travail à partir d'une source de confiance. • Offrir un niveau de sécurité supplémentaire en cas de vol. • Protéger l'accès non autorisé aux données cryptographiques sensibles stockées dans la puce TPM.
Lien avec :	Lettre du ROCD (LET_23-COCD-0035_mot de passe BIOS)

Déclaration :	2. Démarrage sécurisé
Précisions :	
La fonction de démarrage sécurisé (« Secure Boot ») du BIOS doit être activée. Elle permet de vérifier, au démarrage de l'ordinateur, que le système d'exploitation est signé numériquement par un certificat approuvé par le manufacturier. Si les signatures sont valides, le poste de travail démarre et le microprogramme donne le contrôle au système d'exploitation. Le démarrage sécurisé a donc pour but de protéger le poste de travail de l'introduction de code malveillant dans le processus de démarrage (« bootkit » ou « rootkit »). Ainsi, si du code malveillant est introduit dans la séquence de démarrage, le poste de travail ne démarrera plus. **Note :** Le démarrage sécurisé est une norme développée par des fabricants d'ordinateurs pour s'assurer qu'un appareil démarre en utilisant uniquement des logiciels approuvés par le fabricant. Les certificats utilisés pour valider la signature des logiciels de démarrage sont gérés par les manufacturiers et intégrés directement dans le BIOS.	
Justification :	• Empêcher le chargement de logiciel malveillant. • Garantir l'intégrité du processus de démarrage. • Augmenter la confiance à l'intégrité du système d'exploitation. • Protèger des attaques par remplacement du chargeur d'amorçage (rootkit).

Déclaration :	3. Chiffrement des disques
Précisions :	
Mettre en œuvre la fonctionnalité de chiffrement de disques sur les postes de travail afin de protéger les données au repos sur des volumes entiers. Si l'ordinateur possède une technologie TPM (ou équivalent) vous devez obligatoirement utiliser celle-ci afin de procéder au chiffrement des disques de manière sécuritaire. Un processus de sauvegarde des clés de récupération doit également être mis en place afin de pouvoir déverrouiller le disque en cas d'oubli ou de perte de la clé principale. De plus, des mécanismes permettant de vérifier le statut du chiffrement sur l'ensemble des postes de travail doivent être prévus.	
Justification :	Se prémunir contre la fuite d'information, le vol de données, l'accès malintentionné et l'exposition d'appareils perdus, volés ou mis hors service de manière inappropriée.
Lien avec :	Exigence sur le chiffrement des équipements informatiques portables corporatifs Lettre du ROCD (LET_23-COCD_Chiffrement des portables)

Déclaration :	**4. Vérrouillage de session**
Précisions :	
Un mot de passe, ou code confidentiel, doit être exigé avant d'autoriser l'accès à la session de travail d'un utilisateur sur un poste de travail, conformément aux critères suivants : • **Poste joint à un domaine Active Directory :** Les utilisateurs doivent saisir le mot de passe associé à leur compte de domaine lors de l'ouverture ou le déverrouillage de leur session. • **Poste non joint à un domaine Active Directory :** Les utilisateurs doivent saisir un code confidentiel pour accéder à leur session de travail. Ce code confidentiel doit avoir une longueur minimale de six caractères et respecter les exigences de complexité établies. Le verrouillage de session doit également être activé après un délai d'inactivité de 5 minutes et être couplé à un écran de veille qui masque les informations des applications. Pour déverrouiller l'écran de veille, l'utilisateur doit fournir un mot de passe ou un code confidentiel pour pouvoir à nouveau accéder à sa session de travail. Une exception est toutefois permise pour les postes de travail utilisés dans des environnements de soins de santé spécifiques, tels que les blocs opératoires, les laboratoires et les services d'urgence. Peut donc être exclu de cette exigence tout poste de travail utilisé en mode « kiosque » qui respecte les conditions suivantes : • Les applications et les actions autorisées dans ces applications sont limitées aux fonctions spécifiques associées à l'exercice des fonctions requérant l'utilisation du mode kiosque. L'accès aux données sensibles des usagers doit être limité autant que possible. • Les permissions accordées à ces comptes utilisateurs sont restreints et limités dans le respect du principe « besoin de savoir » selon lequel un utilisateur n'a accès qu'à l'information qu'il a besoin dans le rôle ou la fonction qu'il occupe au sein de l'organisation. • L'accès physique à ces postes de travail est strictement limité au personnel de la santé autorisé à y accéder. Cette exception vise à permettre un accès rapide aux informations médicales essentielles dans des situations critiques tout en maintenant un niveau de sécurité élevé des actifs infromationnels.	
Justification :	• Prévenir la fuite de données sensibles. • Réduire le risque de compromission des ordinateurs et des compte utilisateurs. • Se prémunir contre les accès illicites pendant l'absence de l'utilisateur.

Déclaration :	**5. Pare-feu Système**
Précisions :	
Le pare-feu système des postes de travail doit être activé afin de bloquer toute connexion entrante provenant d'appareils situés à l'extérieur du réseau de l'organisation et qui n'a pas été initiée par l'utilisateur ou par le système lui-même. Plus spécifiquement, le pare-feu doit être activé lorsque le poste de travail est directement connecté : • à Internet; • au réseau sans-fil du domicile de l'employé; • à un réseau public tel qu'un cybercafé ou un aéroport. Aucun service ne doit être accessible depuis Internet sur un poste de travail, y compris les connexions de type bureau à distance (RDP).	
Justification :	Minimiser les risques de sécurité en limitant l'exposition des systèmes aux menaces extérieures.

Déclaration :	**6. Sécuriser les comptes administrateurs locaux via LAPS**
Précisions :	
Les comptes administrateur doivent être sécurisés avec le service LAPS (Local Administrator Password Solution). Cette solution génère et sauvegarde automatiquement un mot de passe unique et robuste pour le compte administrateur local des postes dans Active Directory (AD) ou dans Azure Active Directory (AAD). Les paramètres suivants doivent être respectés : • La durée d'expiration des mots de passe ne doit pas dépasser 30 jours; • La longueur des mots de passe être de 14 caractères ou plus; • Les mots de passe doivent inclure des majuscules, minuscules, chiffres et caractères spéciaux.	
Justification :	Réduire les risques de détournement des comptes à privilèges élevés et d'escalade de privilèges.
Lien avec :	Guide d'accompagnement du CESS pour le déploiement de LAPS. Lettre du ROCD (LET_23-COCD-0030_LAPS)

Déclaration :	**7. Détection avancée et réponse aux logiciels malveillants (EDR)**
Précisions :	
Les postes de travail doivent bénéficier d'une version à jour d'un antivirus de nouvelle génération (EDR) qui permet la détection avancée et la réponse automatisée aux activités malveillantes. Le but d'un EDR est de détecter les attaques potentiellement plus avancées que ce que peuvent détecter les antivirus traditionnels, en optimisant le temps de réponse à un incident, en réduisant le taux de faux positifs, en bloquant les menaces avancées et en protégeant le réseau de menaces multiples et agissant simultanément via différents vecteurs d'attaques. Les fonctions suivantes doivent être activés dans l'EDR : • La protection avancée contre les rançongiciels afin de détecter et bloquer l'exécution des fichiers ayant un comportement ressemblant à un rançongiciel; • La protection en temps réel et la mise à jour automatique des signatures de sécurité; • La protection des paramètres de configuration contre les falsifications (« Tamper protection »); • La protection contre les menaces web (« Web Threat Protection ») pour bloquer l'accès aux sites d'hameçonnage, aux sites de mauvaise réputation ainsi qu'aux sites blacklistés.	
Justification :	• Détecter et répondre aux incidents de sécurité. • Limiter l'action et la propagation des logiciels malveillants. • Protéger les paramètres de configuration de l'outil EDR contre les falsifications. • Bloquer l'accès aux site web malicieux.
Lien avec :	Directive sur la cybersécurité – MSSS-DIR03

Déclaration :	8. Filtrage du contenu web
Précisions :	
Le filtrage du contenu web (« Web Content Filtering ») doit être activé afin de bloquer les catégories suivantes : • non catégorisés (« Uncategorized »)[1]; • piratage; • logiciels illégaux. Le filtrage du contenu web permet de suivre et de réglementer l'accès aux sites web en fonction de leurs catégories de contenu. Le blocage d'une catégorie empêche les utilisateurs d'accéder aux URL associées à cette catégorie.	
Justification :	Bloquer l'accès aux site web potentiellement malicieux.
Lien avec :	Directive sur la cybersécurité – MSSS-DIR03

Déclaration :	9. Restriction des périphériques amovibles de stockage
Précisions :	
Les postes de travail doivent être configurés de manière à empêcher l'accès aux périphériques de stockage amovible tels que les clés USB et les cartes Secure Digital (SD). Toute demande d'accès doit être géré par exception et autorisé par le COMSI de l'organisation. Il s'agit également d'empêcher l'exécution de fichiers exécutables (tels que .exe, .dll ou .scr) non signés ou non approuvés à partir de ces périphériques amovibles lorsque leur accès est autorisé via une exception. Cette restriction peut être implémentée via les règles de réduction de la surface d'attaque de votre EDR. Pour encadrer le tout, il est recommandé de mettre en place des exigences d'utilisation des périphériques externes tels que les clés USB. Ces exigences doivent inclure les autorisations d'accès, les cas d'usages, les procédures d'approbation ainsi que les mesures de sécurité associées.	
Justification :	• Limiter la propagation et l'exécution de logiciels malveillants. • Prévenir la perte, le vol de données et l'exfiltration de données.
Lien avec :	Lettre du ROCD (LET_23-COCD-0029_périphériques amovibles)

[1] Le filtrage des accès à Internet doit exclure par défaut la catégorie « Non catégorisé » (unrated ou uncatégorized).

Déclaration :	**10. Protection contre les menaces dans le navigateur web**
Précisions :	
La fonction de détection et de blocage des URL et des sites web malicieux doit être activée dans le navigateur du poste de travail. Cette fonction permet notamment de : • bloquer les attaques par hameçonnage ou les tentatives de distribution de logiciels malveillants via une attaque d'ingénierie sociale; • protéger les mots de passe contre l'hameçonnage; • se prémunir contre l'utilisation dangereuse, par l'utilisateur, d'applications et de sites douteux. Cette fonctionnalité est disponible sur les postes de travail Windows sous le nom « Microsoft Defender Smart Screen » et permet de protéger autant Microsoft Edge que Google Chrome.	
Justification :	Fournir une couche supplémentaire de défense contre l'hameçonnage, les fichiers et applications malveillantes dans les navigateurs web.
Lien avec :	Directive sur la cybersécurité - MSSS-DIR03

Déclaration :	**11. Contrôle des extensions du navigateur web**
Précisions :	
Les extensions installées dans le navigateur web doivent être contrôlées afin de détecter les extensions malveillantes qui, par exemple, volent les données de l'utilisateur comme son identifiant et son mot de passe lorsque celui-ci ouvre une session dans une application web. Il n'est pas nécessaire de bloquer l'installation des extensions, mais au moins être en mesure de détecter qu'une extension malveillante est installée dans le navigateur web d'un poste et d'avoir mis en place un processus pour remédier rapidement à la situation.	
Justification :	Protéger les utilisateurs contre les extensions malveillantes installées à leur insu.
Lien avec :	Guide d'accompagnement du CESS

Déclaration :	**12. Désactivation du compte invité**
Précisions :	
Tout compte invité sur un poste de travail est proscrit. De part sa nature, un compte invité peut facilement être exploité par un individu malveillant afin d'exfiltrer les données du poste de travail ou utilisé comme point d'entrée pour exploiter d'autres vulnérabilités. Par conséquent, le compte invité par défaut du système, généralement sans mot de passe, doit être désactivé sur l'ensemble du parc informatique de l'organisation.	
Justification :	Réduire les risques d'accès non autorisé en désactivant les comptes inutilisés.

Déclaration :	**13. Synchronisation de l'horloge**
Précisions :	
Les postes de travail doivent être configurés pour utiliser le serveur de temps du domaine Active Directory comme source de temps principal. La synchronisation de la date et de l'heure doit être réalisée de manière automatique et périodique afin de maintenir un temps uniforme à travers l'organisation. La synchronisation précise de la date et de l'heure est essentielle pour maintenir la sécurité et l'intégrité des systèmes informatiques. Elle facilite la corrélation des événements suite à un incident de sécurité et garantit la fiabilité de l'horodatage des journaux. La synchronisation du temps est également requise pour le bon fonctionnement du protocole d'authentification Kerberos.	
Justification :	• Faciliter la corrélation des événements de sécurité. • Garantir le bon fonctionnement du processus d'authentification.

Déclaration :	**14. Chiffrement des connexions Bureau à distance (RDP)**
Précisions :	
Toutes les connexions RDP établies vers les postes de travail de l'organisation doivent être configurées de manière à utiliser un chiffrement fort et sécurisé. Le chiffrement doit être activé afin de protéger la confidentialité et l'intégrité des données transmises via ce type de connexion.	
Justification :	Empêcher toute interception non autorisée des mots de passe et des données.

Déclaration :	**15. Destruction des données à la fin de vie du poste de travail**
Précisions :	
Des mesures doivent être prises à la fin de la vie utile d'un poste de travail afin de garantir que toutes les données précédemment stockées sur ce poste sont irrécupérables et définitivement inaccessibles. Plusieurs méthodes peuvent être utilisées pour atteindre cet objectif, notamment : • la destruction physique du disque dur; • l'effacement sécuritaire complet et irréversible de toutes les données stockées sur le poste, sur les clés USB ou sur tout autre support de stockage; • l'effacement sécuritaire des clef de chiffrement des données des disques durs.	
Justification :	Garantir que les données sensibles ne tombent pas entre de mauvaises mains lors du recyclage ou de la réaffectation des postes de travail.