CONSEIL SUPÉRIEUR DU NOTARIAT

Exigences de sécurité pour les postes de travail

Version 1.0 du 23/04/2024

Les exigences suivantes qui sont issues des recommandations de l'ANSSI[1], de la CNIL[2], de *Microsoft*[3] et du *CIS Benchmarks*[4] doivent être respectées dans un délai maximal de 6 mois après leur publication, quel que soit le poste de travail Windows utilisé au sein du notariat.

I. Usage des postes

EXG-SEC-PDT01 : Le poste de travail **doit** être restreint à des usages professionnels et ne doit pas être utilisé à des fins personnelles. Il ne doit pas par ailleurs être utilisé pour réaliser des activités de développement logiciel ou être utilisé comme serveur (Exemple : serveur FTP, serveur Web IIS, serveur MySQL, serveur KMS, etc.).

II. Sécurité physique

EXG-SEC-PST02: Les postes de travail portables **doivent** être fixés au mobilier au moyen d'un câble antivol.

EXG-SEC-PST03: Les postes de travail portables **doivent** disposer d'un filtre écran en situation de mobilité.

III. Configuration BIOS ou UEFI

EXG-SEC-PDT04 : L'accès au microprogramme BIOS ou UEFI du poste **doit** nécessiter un mot de passe robuste respectant les recommandations de l'ANSSI et de la CNIL[5].

EXG-SEC-PDT05 : Le microprogramme BIOS ou UEFI du poste **doit** être configuré de sorte à n'autoriser le démarrage du système *Windows* que depuis le disque dur local au poste, à l'exclusion de tout autre périphérique USB ou depuis un réseau externe (exemples : PXE - *Pre-boot Execution Environment*, *HTTPS Boot*, …).

[1] *Cf.* https://cyber.gouv.fr/publications?field_type_de_publication_target_id%5B934%5D=934
[2] *Cf.* https://www.cnil.fr/fr/securite-securiser-les-postes-de-travail
[3] *Cf.* https://learn.microsoft.com/en-us/windows/security/
[4] *Center for Internet Security* https://www.cisecurity.org/cis-benchmarks
[5] *Cf.* https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

EXG-SEC-PDT06 : Le microprogramme BIOS ou UEFI du poste **doit** être configuré de sorte à utiliser le mécanisme de sécurité *SecureBoot* qui protège contre la falsification du démarrage du poste.

EXG-SEC-PDT07 : Le microprogramme BIOS ou UEFI du poste **doit** être configuré de sorte à activer la puce de sécurité TPM pour qu'elle soit utilisée par le système d'exploitation pour le stockage de secrets.

IV. Socle applicatif

EXG-SEC-PDT08 : Dans le but de maîtriser le socle applicatif et de garantir l'intégrité et la confidentialité des actes électroniques, les progiciels métiers installés sur les postes de travail (hors produits *Microsoft*, composants de base tels que *Acrobat* ou l'agent de télédistribution, ainsi que les outils de la profession pour les services régaliens) **doivent** disposer d'un agrément du CSN ou d'un label Etik.

EXG-SEC-PDT09 : L'installation d'applications tierces (hors produits *Microsoft*) sur le poste de travail **doit** être restreinte et effectuée depuis une source de confiance (Exemple : MECM, Intune, Windows App Store,…). L'utilisateur ne doit pouvoir installer lui-même des applications que si elles ont été préalablement contrôlées et validées dans un magasin d'applications par l'administrateur du poste de travail. Dans le cas contraire, seul l'administrateur du poste doit être capable d'installer une application tierce. Les mécanismes d'auto-élévation de privilèges lors de l'installation d'une application sont interdits.

V. Mises à jour des postes

EXG-SEC-PDT10 : Il est **recommandé** de maintenir à jour la version du microprogramme BIOS ou UEFI des postes de travail, en particulier si des correctifs de sécurité sont publiés.

EXG-SEC-PDT11 : La version de Windows utilisée sur un poste de travail **doit** être supportée par *Microsoft*. A défaut, le poste ne pourra pas se connecter aux services régaliens hébergés par l'ADSN ou le CSN.

EXG-SEC-PDT12 : Le système Windows **doit** être configuré de sorte à installer les mises à jour de sécurité de manière automatique une fois par mois depuis une source de confiance (Exemple : serveurs WSUS pour les moyens et grands offices ou directement depuis les serveurs de mises à jour *Microsoft* pour les petits offices). Les utilisateurs ne doivent pas être capables d'empêcher l'application des mises à jour.

EXG-SEC-PDT13 : Les mises à niveau du système d'exploitation *Windows* **doivent** être maîtrisées et soumises à la validation d'un administrateur.

EXG-SEC-PDT14 : Les logiciels installés sur le poste (*Office* et *Acrobat* en particulier) **doivent** être configurés pour que les mises à jour de sécurité se fassent automatiquement dès que cela est possible.

EXG-SEC-PDT15 : Les mises à jour des bases antivirales (signatures et moteur de détection) **doivent** être effectuées régulièrement.

EXG-SEC-PDT16 : Le poste de travail **doit** être relié à une source et une référence de temps fiable en utilisant le protocole NTP pour la mise à jour de son horloge.

EXG-SEC-PDT17 : Les autorités de certification installées sur les postes de travail et les listes de révocation de certificats (CRL) **doivent** être mis à jour régulièrement.

VI. Gestion des comptes et des autorisations

EXG-SEC-PDT18 : L'ouverture de session utilisateur (même en sortie d'hibernation ou de veille du poste) **doit** utiliser un identifiant personnel propre à l'utilisateur et nécessiter un mot de passe robuste[6], avec une politique de mot de passe respectant *a minima* les règles suivantes :

- Être modifié tous les 180 jours ;
- Ne pas être identique aux 12 derniers mot de passe ;
- Une longueur minimum de 12 caractères ;
- Une complexité exigée comprenant les 4 catégories suivantes :
    - Caractères majuscules (A à Z)
    - Caractères minuscules (a à z)
    - Chiffres en base 10 (0 à 9)
    - Caractères spéciaux (par exemple, !, $, #, %,*)

EXG-SEC-PDT19 : Dans le cas de l'utilisation d'un domaine Active Directory, il est **recommandé**, pour les utilisateurs disposant d'une clé REAL, que l'authentification sur le poste de travail repose le certificat présent sur la carte pour l'ouverture de session (*smartcart logon* exclusif) à condition que le mot de passe ne soit plus nécessaire pour accéder aux applications (l'authentification pour l'accès aux applications doit alors utiliser soit l'authentification *kerberos*, soit le certificat présent sur la clé REAL). Les autres modes d'authentification pour l'ouverture de session (code PIN sans clé, biométrie, …) sont à proscrire.

EXG-SEC-PDT20 : Les règles de sécurité suivantes **doivent** être appliquées à la gestion des sessions utilisateurs du poste :

- L'utilisation de comptes personnels *Microsoft* est interdite ;

---

[6] *Cf.* les recommandations relatives à l'authentification multi-facteurs et aux mots de passe : https://cyber.gouv.fr/publications/recommandations-relatives-lauthentification-multifacteur-et-aux-mots-de-passe

- Le compte invité doit être désactivé ;
- Un mécanisme de verrouillage automatique de session est activé en cas de non-utilisation du poste pendant 15 minutes ;
- Le nombre de tentatives de saisies du mot de passe est limité dans le temps ;
- Le processus de réinitialisation d'un mot de passe pour un compte local ne doit pas s'appuyer sur la simple réponse à des questions de sécurité ;
- Lorsque le poste est joint à un domaine Active Directory, le cache d'authentification ne doit conserver qu'au maximum 4 identifiants.

EXG-SEC-PDT21 : Si le poste de travail est joint à un domaine Active Directory, la gestion du compte d'administration local du poste utilisateur **doit** s'appuyer sur la fonctionnalité *LAPS* pour garantir la rotation des secrets et prévenir de l'usage d'un secret unique disséminé sur de multiple postes utilisateurs.

EXG-SEC-PDT22 : Si le poste de travail est joint à un domaine Active Directory, le secret du compte machine **ne doit pas** pouvoir être modifié et doit subir une rotation tous les 30 jours.

EXG-SEC-PDT23 : Les droits des utilisateurs sur le système Windows **doivent** être limités au strict minimum en fonction de leurs besoins. En aucun cas les droits des utilisateurs ne peuvent être les mêmes que ceux des administrateurs.

VII. Configuration réseau des postes

EXG-SEC-PDT24 : Un « pare-feu » (« *firewall* ») logiciel **doit** être installé et activé sur le poste. L'ouverture des ports de communication pour les flux entrants sur le poste doit être limitée à ceux strictement nécessaires au bon fonctionnement des applications installées sur le poste de travail. Dans le cas où le pare-feu natif du poste est préféré, s'assurer que celui-ci est activé sur le profile « domaine », « privé » et « publique ».

EXG-SEC-PDT25 : En cas d'utilisation du poste de travail à distance, une connexion VPN **doit** être configurée pour accéder automatiquement au réseau interne de l'entité notariale. Une solution VPN utilisant le protocole *Ipsec* de type *Microsoft Always-On* doit être préférée. Pour les offices, la connexion VPN utilisée doit être celle du réseau de l'opérateur agréé.

EXG-SEC-PDT26 : Le poste de travail **ne doit pas** pouvoir être utilisé pour accéder simultanément à des réseaux de confiance différents (Exemple : Internet avec une connexion directe et réseau local de l'office).

EXG-SEC-PDT27 : L'authentification auprès de la borne Wifi **doit** être réalisée à l'aide d'un protocole sécurisé (WPA2 a minima, WPA3 recommandé). Les secrets partagés par plusieurs postes au sein d'un office doivent être renouvelés dans le cas d'un départ d'un collaborateur.

L'usage de certificat personnel sur le poste (différent du certificat présent sur la clé REAL) pour l'authentification au réseau Wifi est recommandé.

EXG-SEC-PDT28 : Le trafic sortant http et https du poste de travail **doit** être acheminé vers un serveur mandataire (*proxy*) sortant afin de garantir que le flux soit contrôlé et filtré. La configuration ne doit pas être modifiable par l'utilisateur.

EXG-SEC-PDT29 : Le poste de travail **ne doit pas** assurer des fonctions de découverte, de routage, de commutation de paquets, de pont ou de point de connexion sans fil.

VIII. Gestion des périphériques

EXG-SEC-PDT30 : La connexion de support amovible USB **doit** être limitée à l'indispensable (clé REAL par exemple). En cas de besoin de transfert de fichiers, une clé sécurisée de type *Datashur* peut être utilisée en n'autorisant que ce type de clé à être connecté sur le poste et en désactivant l'exécution automatique (fonctions « autorun » et « autoplay »).

EXG-SEC-PDT31 : L'installation de nouveaux périphériques (Exemple : imprimantes) **doit** être validée et réalisée par un administrateur.

EXG-SEC-PDT32 : Les communications entre le poste et le ou les périphériques **doivent** être configurées de manière sécurisée (chiffrement et authentification).

IX. Durcissement des postes

EXG-SEC-PDT33 : Les fonctionnalités suivantes **doivent** être désactivées dans l'objectif de prévenir la fuite d'informations :

- localisation du poste de travail ;
- télémétrie et données de diagnostic ;
- identifiant publicitaire, suggestions et suivi du lancement des applications ;
- entrées manuscrites et personnalisation de la saisie.

EXG-SEC-PDT34 : Les utilisateurs des postes de travail **ne doivent pas** pouvoir :

- réaliser des modifications de la configuration du système et désactiver les fonctions de sécurité ;
- charger ou décharger les pilotes de périphérique ;
- exécuter du code *Powershell* ;
- ajouter ou modifier des comptes utilisateurs.

EXG-SEC-PDT35 : Les services suivants **doivent** être désactivés :

- Service de géolocalisation (*lfsvc*)
- Service de diagnostic (*diagsvc*)
- Service de découverte réseau (*lltdsvc*)
- Service d'administration SSH (*sshd*)
- Services de partage administratifs (*lanmanserver*)
- Service développeur (*Wisvc*)
- Service de gestion de sous-système (*LxssManager*)
- Services peer-to-peer (*PNRPsvc*, *p2pimsvc*, *p2psvc*, *p2pimsvc*, *PNRPAutoReg*)
- Service de gestion RPC obsolète (*RpcLocator*)
- Service de gestion UPnP (*upnphost*)
- Service de partage Windows Media (*WMPNetworkSvc*)
- Service de partage de connexion de données cellulaires (*icssvc*)
- Service de routage (*RemoteAccess*)
- Service de supervision (*SNMP*)
- Services de jeux Xbox (*XboxGipSvc*, *XblAuthManager*, *XblGameSave*, *XboxNetApiSvc*)

EXG-SEC-PDT36 : Les règles de sécurité suivantes **doivent** être appliquées aux protocoles utilisés :

- Désactivation du protocole *LLMNR* ;
- Désactivation du protocole *SMB v1* ;
- Signature des communications reposant sur le protocole *SMB* ;
- Désactivation du protocole *Netbios* ;
- Désactivation des protocoles Lan Manager (*LM*) et *NTLM v1*;
- Les connexions RPC entrantes doivent être configurées pour être authentifiées (*Packet Level Privacy*) et chiffrées ;
- Le protocole *WinRM* doit être utilisé de manière sécurisée (authentification et chiffrement).

EXG-SEC-PDT37 : Dans le cas de l'utilisation d'un domaine Active Directory, il est **recommandé** d'utiliser le protocole d'authentification *kerberos*. Le cas échéant, le protocole *NTLM v2* peut être utilisé.

X. Solutions de sécurité

EXG-SEC-PDT38 : La protection antimalware au démarrage (ELAM) **doit** être activée pour garantir la sécurité des pilotes de démarrage chargés par le système d'exploitation.

EXG-SEC-PDT39 : Un antivirus **doit** être activé et installé sur le poste de travail. Sa désactivation par un utilisateur ne doit pas être possible. Il doit être configuré pour une mise en quarantaine des charges malveillantes détectées et la rétention doit être configurée pour une durée

minimale d'un an. L'antivirus ne doit pas avoir de liste d'exclusion incluant des dossiers dans lesquels sont stockés du contenu provenant d'internet (Outlook, navigateur, etc.).

EXG-SEC-PDT40 : La protection anti-sabotage, en temps réel, comportemental et anti-spyware de l'antivirus **doit** être activée. Tout contenu provenant de l'extérieur (navigateurs, pièces jointes, périphérique USB, etc.) doit être scanné par la solution antivirale.

EXG-SEC-PDT41 : Le disque dur du poste de travail **doit** être chiffré avec la fonctionnalité intégrée *Bitlocker* en utilisant le module TPM du poste pour le stockage de la clé. Les options de recouvrement ne doivent pas être configurables par l'utilisateur. Il est recommandé de stocker la clé de recouvrement :

- Dans un coffre-fort pour les postes qui ne sont pas joint à un domaine Active Directory ;
- Au sein de l'Active Directory pour les postes joint à un domaine.

EXG-SEC-PDT42 : Le contrôle d'applications intégré *Applocker* **doit** être activé sur les postes en n'autorisant l'exécution des applications pour les utilisateurs que depuis les répertoires *Programmes* et *Windows* (les administrateurs n'ayant aucune restriction). En cas de besoin spécifique pour des applications qui ne s'installeraient pas dans le répertoire *Programmes*, un répertoire dédié (autre que les répertoires *Utilisateurs* et *Documents*) peut être ajouté ou il est possible de recourir à des règles spécifiques permettant d'autoriser des logiciels signés par une autorité de certification reconnue.

EXG-SEC-PDT43 : Le contrôle de compte utilisateur (*UAC*) **doit** être activé et une élévation de privilèges doit être systématiquement soumise à une demande de consentement de l'utilisateur et à une saisie des identifiants et mots de passe nécessaires à l'obtention des privilèges demandés.

EXG-SEC-PDT44 : L'élévation de privilèges **doit** être demandée systématiquement lors de l'installation d'applications ou de périphériques (Exemple : imprimante).

EXG-SEC-PDT45 : Afin de prévenir des attaques de bouclage, la restriction du contrôle de compte utilisateur (UAC) à distance **doit** être systématiquement activée.

EXG-SEC-PDT46 : Le mode d'approbation de l'administrateur **doit** être configuré pour qu'une demande de consentement soit systématiquement demandée lors de l'usage du compte administrateur.

EXG-SEC-PDT47 : Il est **recommandé** d'activer les fonctionnalités de sécurité suivantes en fonction de leur disponibilité dans la licence Windows utilisée et de leur compatibilité matérielle des postes de travail :

- Activer les fonctionnalités de sécurité basées sur la virtualisation (*Virtualization based security*) ;

- Activer *Credential Guard* et le mode protégé pour assurer la sécurité des secrets stockés dans la base LSASS des systèmes d'exploitation ;
- Activer *Device Guard* pour protéger contre une exécution de code malveillante ;
- Activer *Exploit Guard* pour les moyens et grands offices pour prévenir d'une infection ;
- Activer *SmartScreen* (ou *SafeBrowsing*) et s'assurer que l'utilisateur ne peut pas contourner cette politique ;
- Activer la prévention de l'exécution des données (*DEP*) pour protéger contre le lancement de code exécutable depuis des emplacements considérés comme « non standards » ;
- Activer le mode de consultation protégé pour tous les documents Office provenant de l'extérieur et désactiver l'exécution de macros, lorsque cela est possible ;
- Utiliser un mécanisme de type « bac à sable » lorsque cela est possible et s'assurer que l'isolation avec le système hôte est stricte ;
- Bloquer les applications potentiellement indésirables (PUA).

EXG-SEC-PDT48 : Lorsque les mesures de sécurité issues des exigences précédentes ont été appliquées, l'usage d'une solution de détection de type EDR est **recommandé** sur les postes de travail avec l'usage d'un service de type SOC pour superviser les évènements de sécurité remontés par cette solution.

XI. Journalisation

EXG-SEC-PDT49 : Il est **recommandé** que les journaux des différents postes de travail soient acheminés vers un point de collecte lorsque cela est possible afin de respecter les exigences émises par la CNIL pour garantir l'archivage et faciliter les investigations dans le cadre d'incidents par les autorités compétentes.

EXG-SEC-PDT50 : La journalisation **doit** être activée et les éléments de journalisation suivants doivent être configurés :

- Activer la journalisation des lignes de commandes ;
- Activer, lorsque cela est possible, la journalisation des *hash* des charges identifiées par l'antivirus comme malveillantes ;
- Activer la journalisation du composant *Application Guard* ;
- Activer la journalisation *Powershell* et la journalisation *Powershell Transcript* ;
- Activer la journalisation des authentifications NTLM entrantes ;
- Activer la journalisation des authentifications NTLM sortantes vers des serveurs distants.

EXG-SEC-PDT51 : Seul un administrateur privilégié **doit** pouvoir gérer ou consulter les journaux critiques tels que le journal d'audit ou le journal de sécurité.

EXG-SEC-PDT52 : La taille du journal sécurité **doit** être augmentée à 400 Mo conformément aux recommandations de l'ANSSI[7] pour garantir la rétention des traces pendant une durée suffisante dans le but de faciliter les investigations numériques.

XII. Sauvegarde et gestion des données

EXG-SEC-PDT53 : Le stockage des données métiers des utilisateurs **doit** être effectué sur un espace de stockage régulièrement sauvegardé, accessible via le réseau interne de l'office plutôt que sur les postes de travail. Dans le cas où des données sont stockées localement, des moyens de synchronisation ou de sauvegarde aux utilisateurs doivent être fournis et utilisés.

EXG-SEC-PDT54 : Les données de configuration des postes de travail, incluant les sources d'installation, les licences et les fichiers de configuration des applications, **doivent** être sauvegardées.

EXG-SEC-PDT55 : La fréquence des sauvegardes des données métiers (présentes sur le poste de travail) **doit** *a minima* être hebdomadaire et celle des données de configuration *a minima* mensuelle.

EXG-SEC-PDT56 : Il est **recommandé** d'appliquer la règle simple « 3-2-1 » : 3 copies de sauvegarde, sur 2 supports différents dont 1 hors ligne qui peut être par exemple sur un support physique comme un disque dur externe chiffré ou stocké dans un lieu sécurisé.

EXG-SEC-PDT57 : Les sauvegardes **doivent** faire l'objet de tests réguliers de restauration pour garantir qu'elles seront exploitables le moment venu (par exemple après un incident de sécurité majeur de type attaque par rançongiciel).

EXG-SEC-PDT58 : Les données présentes sur les postes de travail **doivent** être effacées de manière sécurisée[8] préalablement à sa réaffectation à un autre utilisateur ou en cas de mise au rebut du poste.

XIII. Administration

EXG-SEC-PDT59 : En cas d'utilisation de solution d'assistance à distance sur le poste, celle-ci **ne doit pas** être possible depuis Internet sans utilisation préalable de solution de type VPN avec authentification forte. Les outils d'administration à distance doivent par ailleurs recueillir l'accord

[7] Cf. les recommandations de sécurité pour la journalisation d'un système Microsoft : https://cyber.gouv.fr/publications/recommandations-de-securite-pour-la-journalisation-des-systemes-microsoft-windows-en

[8] *Cf.* https://cyber.gouv.fr/sites/default/files/document/anssi-guide-reconditionnement_ordinateurs_bureau_portables_v1-0.pdf

de l'utilisateur avant toute intervention sur son poste (en répondant par exemple à un message s'affichant à l'écran) et l'utilisateur doit également pouvoir constater si la prise de main à distance est en cours et quand elle se termine (affichage d'un message à l'écran par exemple). Un compte n'ayant pas les droits administrateurs de domaine doit être utilisé pour effectuer la prise en main à distance.

EXG-SEC-PDT60 : Les outils d'administration à distance **doivent** être utilisés de manière sécurisés :

- Les redirections sont interdites (partages, RPC, …) ;
- Le chiffrement des flux doit être réalisé à l'aide de protocoles de chiffrement robustes[5] ;
- Les connexions doivent systématiquement demander un mot de passe ;
- L'authentification au niveau du réseau (NLA) doit être configurée.

EXG-SEC-PDT61 : Les postes de travail utilisés pour l'administration des postes de travail des utilisateurs **ne doivent pas** disposer d'une connexion à Internet directe, que ce soit pour la navigation Web ou la messagerie conformément aux recommandations de l'ANSSI sur l'administration des systèmes[9].

EXG-SEC-PDT62 : Si le poste de travail est joint à un domaine Active Directory :

- Les administrateurs de domaine **ne doivent pas** pouvoir se connecter sur le poste. Des comptes d'administration spécifiques permettant l'administration des postes de travail doivent être utilisés ;
- Les communications avec le ou les contrôleurs de domaine **doivent** être signées et chiffrées ;
- L'administration par GPO est **recommandée** et il convient de s'assurer qu'elles sont systématiquement appliquées à fréquence régulière ;
- Des restrictions sur l'énumération de sessions **doivent** être appliquée (par l'utilisation par exemple du module *NetCease*) pour prévenir de l'usage d'outils de reconnaissance tels que *BloodHound*.

[9] *Cf.* https://cyber.gouv.fr/publications/recommandations-relatives-ladministration-securisee-des-si