Ce document présente une liste complète d'exigences de cybersécurité destinées à renforcer la sécurité des postes de travail. Ces exigences couvrent divers aspects, allant de la sécurité physique à la sécurité logicielle, en passant par la gestion des comptes, la configuration réseau et les procédures d'administration. L'objectif est de fournir un cadre de référence pour la mise en place d'une infrastructure informatique sécurisée et résiliante.
Les exigences suivantes qui sont issues des recommandations de l’ANSSI, de la CNIL, de Microsoft
et du CIS Benchmarks doivent être respectées, quel que soit le poste de travail Windows utilisé au sein du notariat.

Cadre de Sécurité des Postes de Travail

Sécurité Physique

Mesures pour protéger l'accès physique aux postes de travail.

Sécurité Logicielle

Protocoles pour protéger les logiciels contre les menaces.

Gestion des Comptes

Politiques pour gérer et sécuriser les comptes d'utilisateurs.

Configuration Réseau

Paramètres pour sécuriser les connexions réseau.

Procédures d'Administration

Processus pour maintenir et sécuriser les systèmes.

Utilisation des postes de travail et sécurité physique

Caractéristique	Utilisation professionnelle	Sécurité physique	Confidentialité de l'écran
Utilisation	Utilisation professionnelle uniquement	Non applicable	Filtre en situation de mobilité
Serveur	Ne peut pas être un serveur	Non applicable	Non applicable
Prévention du vol	Non applicable	Sécurisé avec un câble antivol	Non applicable

Renforcement du BIOS/UEFI

1

Protéger l'accès au BIOS/UEFI avec un mot de passe robuste. Empêche les modifications non autorisées des paramètres de démarrage.

Protection par mot de passe

2

Configurer le BIOS/UEFI pour démarrer uniquement à partir du disque dur local. Empêche le démarrage à partir de supports externes malveillants.

Démarrage à partir du disque dur local

3

Activer SecureBoot pour garantir que seuls les systèmes d'exploitation et les pilotes de confiance se chargent.

Activation de SecureBoot

4

Activer la puce TPM pour stocker en toute sécurité les clés de chiffrement.

Activation de la puce TPM

Sécurité du socle applicatif

Logiciel approuvé par le CSN

Utiliser uniquement des logiciels approuvés et agréés par le CSN pour garantir la sécurité.

Installation restreinte

Restreindre l'installation de logiciels aux seuls utilisateurs autorisés pour prévenir les logiciels malveillants.

Assurer la sécurité et la stabilité du système grâce à des mises à jour régulières

BIOS/UEFI

Mettre à jour régulièrement le BIOS/UEFI pour la sécurité et la stabilité

Windows

Utiliser une version de Windows supportée pour les mises à jour de sécurité

Mises à niveau

Valider les mises à niveau du système avant déploiement

Maj securité

Activer les mises à jour automatiques de sécurité pour Windows

Maj automatiques

Activer les mises à jour automatiques des logiciels pour la sécurité

Maj antivirus

Mettre à jour régulièrement les définitions antivirus

Maj certificats

Mettre à jour les certificats et les CRL pour l'authentification

Horloge NTP

Synchroniser l'horloge système avec le serveur NTP

Améliorer la sécurité des comptes et des sessions

Droits d'utilisateur limités

Attribuer des droits d'utilisateur limités pour réduire les risques

Identifiants personnels

Exiger des identifiants personnels et des mots de passe robustes pour l'accès des utilisateurs

Rotation des secrets des machines

Faire tourner régulièrement les secrets des machines pour la sécurité

Authentification par certificat

Utiliser des certificats pour une authentification sécurisée

LAPS pour les comptes admin

Gérer les mots de passe des administrateurs locaux avec LAPS

Interdiction des comptes personnels

Interdire l'utilisation de comptes personnels sur les appareils professionnels

Sécurité des mots de passe

Complexité des mots de passe

Les mots de passe doivent inclure des majuscules, des minuscules, des chiffres et des caractères spéciaux.

Rotation des mots de passe

Les mots de passe doivent être modifiés tous les 180 jours pour maintenir la sécurité.

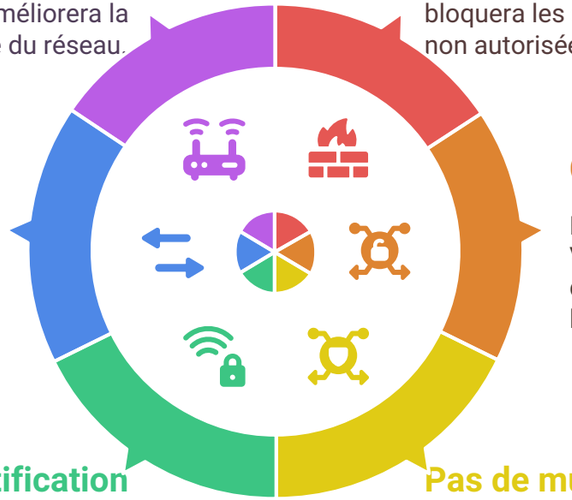
Longueur des mots de passe

Les mots de passe doivent avoir une longueur minimale de 12 caractères.

Unicité des mots de passe

Les mots de passe ne doivent pas être identiques aux 12 derniers utilisés.

Mesures de sécurité réseau



Pas de routage de paquets

Empêcher le routage/commutation de paquets sur les postes de travail. Cela améliorera la sécurité du réseau.

Pare-feu logiciel

Activer le pare-feu logiciel sur chaque poste de travail. Cela bloquera les connexions non autorisées.

Redirection via proxy

Rediriger le trafic HTTP/S via un serveur proxy. Cela filtrera le contenu web.

Connexion VPN

Exiger une connexion VPN pour l'accès à distance. Cela protégera le réseau de l'entreprise.

Authentification Wifi sécurisée

Utiliser une authentification Wifi sécurisée pour protéger l'accès sans fil. WPA2 Enterprise est un exemple.

Pas de multi-accès

Empêcher les postes de travail d'accéder à plusieurs réseaux. Cela évite la propagation des menaces.

Sécuriser les périphériques informatiques

Validation admin

Maintient le contrôle sur l'environnement informatique en exigeant l'approbation pour les nouveaux périphériques.

Limiter les ports USB

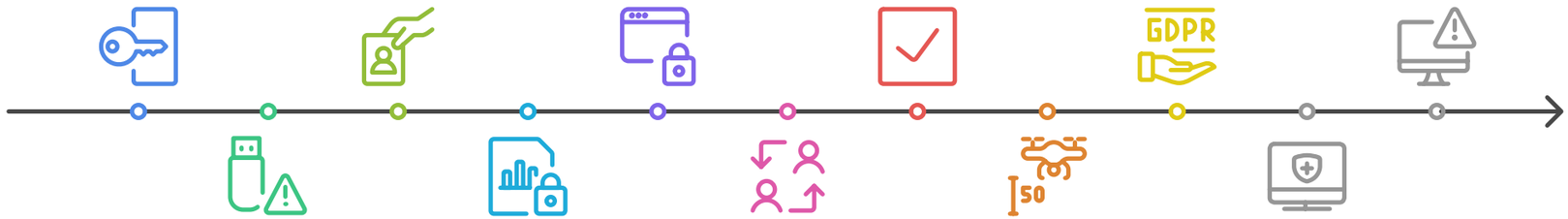
Empêche l'exfiltration de données et les infections par clé USB en autorisant uniquement les périphériques approuvés.

Communication sécurisée

Assure une communication sécurisée des périphériques grâce au chiffrement et à l'authentification.

Sécurité du système

Mesures de sécurité logicielle



Activer ELAM

Protéger le démarrage du système contre les malwares

Activer l'antivirus

Assurer la détection et le blocage des menaces

Utiliser la protection en temps réel

Détecter les menaces inconnues grâce à l'analyse comportementale

Activer le chiffrement du disque

Protéger les données avec BitLocker et TPM

Activer Applocker

Restreindre l'exécution d'applications non autorisées

Activer UAC

Demander une confirmation pour les actions sensibles

Exiger une élévation de privilèges

Bloquer les abus en demandant une authentification

Restreindre l'UAC à distance

Empêcher l'exécution de commandes privilégiées à distance

Exiger le consentement de l'administrateur

Ajouter une couche de validation humaine pour les actions sensibles

Activer les protections avancées

Renforcer la sécurité du noyau système avec VBS et DEP

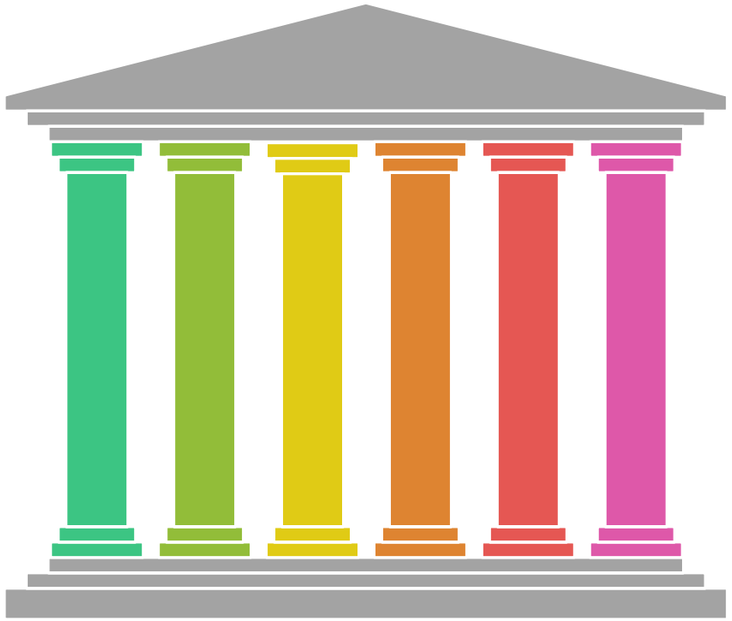
Mettre en œuvre une solution EDR

Surveiller et réagir aux comportements suspects

Configuration de la journalisation

	Point de collecte	Journalisation de sécurité	Journaux critiques administrateurs	Taille jounaux augmentés
Objectif	Surveillance centralisée	Capacité d'audit	Restriction d'accès	Conservation des données
Action	Acheminer les journaux	Activer la journalisation	Limiter l'accès	Augmenter la taille
Objet	Journaux de sécurité	Événements de sécurité	Journaux de sécurité	Journaux de sécurité
Cible	Serveur centralisé	N/A	Administrateurs uniquement	N/A

Stratégies de Sauvegarde des Données



Stockage des Données Métiers

Assurer la sécurité des données critiques de l'entreprise grâce à des sauvegardes régulières.

Sauvegarde de la Configuration

Maintenir des sauvegardes régulières des configurations système pour une restauration rapide.

Fréquence de Sauvegarde

Établir des intervalles de sauvegarde réguliers pour minimiser la perte de données.

Règle 3-2-1

Adhérer à la règle 3-2-1 pour une redondance et une sécurité optimales des données.

Tests de Restauration

Effectuer des tests réguliers pour garantir la fiabilité des sauvegardes.

Effacement Sécurisé des Données

Utiliser des méthodes d'effacement sécurisées pour empêcher la récupération non autorisée.

Stratégies de Sécurité de l'Administration

Assistance à Distance Sécurisée

Utilisation de solutions d'assistance à distance sécurisées pour limiter les risques d'intrusion.

Outils d'Administration Sécurisés

Encadrer l'usage des outils d'administration pour éviter les abus ou erreurs.

Accès Internet Restreint

Interdire l'accès Internet direct depuis les postes d'administration pour éviter les menaces en ligne.

Communication Sécurisée du Contrôleur de Domaine

Sécuriser les échanges entre les contrôleurs de domaine pour préserver l'intégrité de l'Active Directory.