

Cocher CyberFundamentals Basic : la checklist pour un bureau sur Canvos

Le cadre CyberFundamentals du Centre pour la Cybersécurité Belgique est la référence belge pour NIS2 et pour toute organisation qui veut démontrer que les bases sont en ordre. Cette checklist parcourt les mesures du niveau Basic et montre, par mesure, ce que Canvos règle par défaut, ce que vous configurez vous-même et ce qui sort du cadre de l'espace de travail. Avec un PDF imprimable.

Intégré = activé par défaut ou un paramètre · Partiel = demande votre choix ou complément · Votre politique = hors espace de travail

Identifier : savoir ce que vous avez

	Statut	Date	Responsable
☐ Inventaire des utilisateurs et des accès La liste des utilisateurs dans la gestion de l'organisation montre chaque compte avec rôle, statut, stockage et boîte mail. Exportez en CSV pour votre inventaire.	intégré		
☐ Inventaire des appareils Les sessions actives montrent appareil et navigateur par utilisateur. Les ordinateurs et téléphones eux-mêmes restent dans votre propre registre.	partiel		
☐ Inventaire des logiciels et services cloud Canvos remplace mail, fichiers, suite bureautique, chat, réunions et coffre-fort : un fournisseur sur la liste au lieu de six. Les autres logiciels restent à inventorier par vous.	partiel		
☐ Politique et exigences légales Une politique de sécurité de l'information, un registre RGPD des traitements et l'enregistrement NIS2 auprès du CCB. Voir la checklist du registre des traitements.	votre politique		
☐ Risque fournisseur Canvos tourne en Europe avec un fournisseur belge, sans maison mère américaine ; le contrat de sous-traitance et la localisation des données sont fixés.	intégré		

Protéger : accès, données, sauvegarde, sensibilisation

	Statut	Date	Responsable
☐ Identités et authentification forte (MFA) Authentification à deux facteurs avec application ou clé matérielle par utilisateur ; une connexion pour tous les modules.	intégré		
☐ Moindre privilège et rôles Rôles & Apps décident qui voit quel module ; les dossiers d'entreprise donnent des droits par groupe.	intégré		
☐ Accès à distance et mobile Politique mobile : protection d'écran, déverrouillage biométrique, verrouillage automatique. Les sessions peuvent être terminées à distance.	intégré		
☐ Données protégées au repos et en transit TLS partout, sauvegardes chiffrées (AES-256), classification avec étiquettes, DLP sur numéros de registre national et IBAN, politique de partage avec mot de passe et expiration.	intégré		
☐ Sauvegardes réalisées, conservées et testées Sauvegardes quotidiennes chiffrées avec conservation en un paramètre. Le test de restauration annuel, vous le planifiez et le documentez.	partiel		
☐ Configuration de base sûre et correctifs Serveurs, mises à jour et correctifs de sécurité sont gérés par Canvos ; fichiers et pièces jointes exécutables bloqués par défaut.	intégré		

☐	Retrait des accès au départ Désactiver un compte ferme mail, fichiers, agenda, chat et coffre-fort en même temps ; les sessions expirent.	intégré
☐	Sensibilisation et formation Une session annuelle sur le phishing et les mots de passe reste nécessaire. Les guides de ce site peuvent servir de support.	votre politique
☐	Journaux conservés Journal des connexions et événements de gouvernance, hachés et ancrés chaque jour, conservés selon la politique de rétention.	intégré

Détecter : voir ce qui se passe

	Statut	Date	Responsable
☐	Événements collectés et corrélés Chaque action de politique dans la chaîne de preuve ; export en CEF vers un SIEM, ou CSV et JSON.	intégré	
☐	Connexions suspectes Nouveau pays ou nouvelle IP signalés, échecs répétés bloqués temporairement, approbation possible.	intégré	
☐	Code malveillant Fichiers et pièces jointes exécutables bloqués, mail filtré contre spam et malware. La protection des postes de travail reste votre choix.	partiel	
☐	Alertes aux bonnes personnes Alertes en temps réel et rapport de conformité mensuel aux adresses que vous définissez.	intégré	

Répondre : quand ça tourne mal

	Statut	Date	Responsable
☐	Plan d'incident Qui appelle qui, ce qui est notifié au CCB dans les 24 et 72 heures. Une page suffit pour Basic ; gardez-la dans le coffre-fort.	votre politique	
☐	Analyse : que s'est-il passé Journal des connexions et chaîne de preuve reconstituent en minutes qui a partagé ou ouvert quel fichier.	intégré	
☐	Maîtrise Terminer les sessions, désactiver le compte, réinitialiser le mot de passe, conservation légale sur les fichiers concernés.	intégré	
☐	Communication et notification L'export fournit les faits pour la notification ; la notification elle-même et la communication avec les personnes concernées vous reviennent.	partiel	

Rétablir : reprendre le travail

	Statut	Date	Responsable
☐	Restauration depuis la sauvegarde Restaurable par vous-même avec votre propre clé, sans ticket chez un fournisseur.	intégré	
☐	Plan de reprise et test Documentez qui restaure, où se trouve la clé et combien de temps c'est acceptable. Testez au moins une fois par an.	partiel	
☐	Leçons et amélioration Après un incident : que changeons-nous dans la politique et les paramètres ? Le score de conformité montre l'effet immédiatement.	votre politique	

