LABEL CYBER SAFE

Exigences V3.0 – 2023 – Principales nouveautés et modifications

Ce document présente les principales nouveautés apportées aux exigences du Label Cyber-Safe par le groupe «Normalisation» au cours du travail de révision 2022-2023.

Ressources humaines

- La personne responsable de la cybersécurité doit désormais signer et avoir accès aux documents suivants :
  - Inventaire des données,
  - Liste des permissions d'accès,
  - Checklist "Résilience".
- *Pour les PME:* Une séance de présentation des résultats de la campagne de phishing doit avoir lieu, avec une présentation des bonnes pratiques (un PV devra être disponible disponible).
- *Pour les communes et administrations publiques :* tous les employés devront avoir suivi le e-Learning sur la sécurité de l'information et la cybersécurité (e-Learning développé sur mandat de la CCDJP).

Test de phishing

- Le taux de clics est généralement réduit.
- Introduction d'une exigence concernant les téléchargements de contenu à distance.

Chiffrement et authentification

- Tous les systèmes d'authentification accessibles publiquement devront mettre en œuvre l'authentification multi facteur (a minima VPN, le RDP, webmail, les services de partage de documents type Sharepoint).

Procédures, routines

- Toutes les macros devront être désactivées par défaut dans les logiciels de bureautique ou auront un accès restreint.

Procédures, routines

- Le filtrage (anti-spam) et l'anti-spoofing (SPF et DKIM) devront être activés pour toutes les adresses électroniques.

Sauvegardes

- Le bon fonctionnement de la sauvegarde système devra être vérifié au moins tous les trois mois.

Résilience

- L'organisation candidate devra remplir et signer la liste de contrôle "Résilience".