الوكالة الوطنيّة للسّلامة المعلوماتيّة

Agence Nationale de la Sécurité Informatique

Guide de bonnes pratiques

« La mise en œuvre d'un environnement sécurisé de télétravail »

Janvier 2023

Version 1.0

Guide de bonnes pratiques

« La mise en œuvre d'un environnement sécurisé de télétravail »

A- Politique de télétravail

- Elaborer et mettre à la disposition de l'employé un document qui décrit les règles, les conditions et les restrictions d'autorisation du télétravail conformément à la norme **ISO 27002 : Sécurité de l'information, Cybersécurité et protection de la vie privée - Mesures de la sécurité de l'information**.
- Elaborer ou mettre à jour les procédures métiers pour prendre en considération les exigences du télétravail.
- Procéder à la révision de la dite documentation périodiquement et suite à tout changement de l'environnement métier.

B- Equipement d'accès : postes de travail, Smartphones, tablettes, etc.

- Fournir un équipement sécurisé (poste de travail, Tablette, etc.) conformément à la politique de la sécurité de l'information de l'entreprise.
- Installer le client de la solution anti-virus déployée par votre entreprise pour assurer la mise à jour régulière et le contrôle continu des anomalies lors de la connexion au réseau de votre entreprise via VPN.
- Mettre à jour périodiquement les systèmes d'exploitation et les applications installées pour assurer la correction des dernières vulnérabilités.
- Utiliser un compte utilisateur limité lors de l'accès au réseau de votre entreprise et l'interdire d'installer des applications sans l'autorisation du RSSI.
- Utiliser des mots de passe robustes (**guide mot de passe**).
- Installer le client de votre solution VPN depuis la source officielle.
- Mettre en œuvre une solution de chiffrement de disque.
- Crypter vos données strictement confidentielles.
- Scanner immédiatement tout support amovible avant utilisation.
- S'assurer de la sécurité du réseau domestique de l'employé.

C- Accès au réseau et aux applications métiers de l'entreprise

- Accéder au réseau d'entreprise seulement via un tunnel VPN sécurisé avec chiffrement du trafic.
- Utiliser des mots de passe robustes pour les comptes VPN.
- Réaliser un filtrage sur les applications accessibles via le tunnel VPN.
- Mettre en place une zone DMZ entrante pour les accès VPN aux applications métiers de l'entreprise et éviter de les exposer directement sur Internet.
- Réviser la matrice d'accès de l'employé concerné par le télétravail aux applications métiers.

- Activer si possible l'authentification multi-facteur aux applications métiers de l'entreprise.
- Configurer le Firewall conformément à la matrice d'accès révisée.

D- Journalisation, Prévention et Détection des intrusions

- Activer la journalisation des événements pour tous les équipements intervenant au télétravail (équipement d'accès, anti-virus, routeurs, Firewall, etc.)
- Superviser les flux de télétravail au moyen d'une solution de prévention, détection d'intrusions (IPS, IDS).
- S'assurer de la synchronisation horaire de tous les équipements intervenant au télétravail.

E- Sauvegarde

- Sauvegarder régulièrement vos données conformément à la politique et à la procédure de sauvegarde et de continuité d'activité de votre entreprise.

F- Solution de visioconférence

- Opter pour une solution de visioconférence fiable.
- Activer l'authentification multi-facteurs aux utilisateurs.
- S'assurer du chiffrement des communications de bout en bout.
- Réaliser des réunions en ligne en mode privé, les protéger à l'aide d'un mot de passe.
- Avant le démarrage d'une réunion en ligne, configurer une salle d'attente virtuelle qui permettra de vérifier la fiabilité des participants potentiels.

G- Sensibilisation et formation de l'employé

- Prévoir des sessions de sensibilisation face aux risques liés au télétravail (Phishing, vol de données, les ransomwares, etc.) et de formation le cas échéant pour les employés concernés par le télétravail.
- Exiger la signature d'une charte de télétravail par les employés concernés.