Télétravail

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

**6. Exigences de la norme ISO 27001 : 2022**

**7. Politique télétravail**

Historique

|  |  |  |
| --- | --- | --- |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
| Toutes | Création | 01/01/2022 |
| **Page** | **Changement** | **Date** |

**1. Objet**

La politique télétravail a pour objet de décrire les règles et exigences du télétravail.

**2. Finalité**

La politique télétravail a pour finalité d’assurer la sécurité de l’information quand le personnel travaille à distance.

**3. Domaine d’application**

La politique télétravail s’applique à toute personne travaillant en dehors des locaux de l’organisation (à leur domicile ou en déplacement temporaire).

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique télétravail. Il est garant de son application. Il a l’appui du directeur et des départements concernés.

**5. Documents**

Sécurité pour le télétravail

Déclaration des événements

Transfert de l’information

Authentification

Programmes utilitaires privilégiés

Bureau propre et écran vide

Sauvegarde

Continuité d’activité

**6. Exigences de la norme ISO 27001 : 2022**

A.6.7 Télétravail

Des mesures de sécurité doivent être mises en œuvre lorsque le personnel travaille à distance, pour protéger les informations accessibles, traitées ou stockées en dehors des locaux de l'organisation.

**7. Politique télétravail**

Le travail à distance (télétravail) se produit lorsque le personnel de l'organisation travaille à partir d'un emplacement en dehors des locaux de l'organisation, accédant à des informations sur papier ou par voie électronique via un équipement TIC (technologie de l’information et de la communication).

Le télétravail présente de nouveaux risques relatifs à la confidentialité et la sécurité de l’information.

La politique télétravail établit les conditions et restrictions pertinentes et prend en compte les éléments suivants :

* la sécurité physique existante du site de travail à distance, son emplacement et environnement local, cf. le fichier Sécurité pour le télétravail
* les règles et mécanismes de sécurité comme :
  + armoire de classement à clé
  + transport sécurisé
  + règles d'accès à distance
  + bureau dégagé
  + impression et élimination sécurisés
  + signalement des événements de sécurité de l'information selon la procédure Déclaration des événements
* les exigences de sécurité des communications selon la procédure Transfert de l’information, en tenant compte de la :
  + nécessité d'un accès à distance aux systèmes de l'organisation
  + sensibilité de l’information
  + sensibilité des systèmes et des applications
* l'utilisation d'un accès à distance (bureau virtuel) qui prend en charge le traitement et le stockage de l'information sur un équipement privé
* la menace d'un accès non autorisé à l’information par d'autres personnes :
  + sur le site de travail à distance (famille, amis)
  + dans des lieux publics
* l'utilisation des réseaux domestiques et des réseaux publics et les exigences et restrictions sur la configuration des services de réseau sans fil
* l'utilisation de mesures de sécurité (pare-feu, protection contre les logiciels malveillants)
* des mécanismes sécurisés pour :
  + le déploiement et l'initialisation des systèmes à distance
  + l'authentification et l'activation des d'accès privilégiés en tenant compte de la vulnérabilité des moyens d'authentification à facteur unique selon les procédures Authentification et Programmes utilitaires privilégiés

Le télétravail tient compte des éléments suivants :

* la fourniture d'équipements et de meubles de stockage appropriés (interdiction d’utiliser des équipements privés qui ne sont pas sous le contrôle de l'organisation)
* la définition du domaine d’application du travail autorisé
* la classification de l’information pouvant être détenue
* les systèmes et services internes auxquels un accès est autorisé
* la formation des personnes travaillant à distance (comment travailler de manière sécurisée)
* la fourniture d'équipements de communication appropriés :
  + sécurisation de l'accès à distance
  + exigences relatives au verrouillage de l'écran selon la politique Bureau propre et écran vide
  + activation du suivi de l'emplacement de l'appareil
  + installation de capacités d'effacement à distance
* la sécurité physique
* les règles et conseils sur l'accès de la famille et des visiteurs aux équipements et à l’information
* la fourniture d'assistance et de maintenance matérielle et logicielle
* la fourniture d'assurance
* les activités de sauvegarde et de continuité d'activité selon les procédures Sauvegarde et Continuité d’activité
* la surveillance et l’audit de la sécurité
* la révocation de l'autorité et des droits d'accès et la restitution du matériel lorsque les activités de travail à distance sont terminées

Les conditions et restrictions pour la Sécurité pour le télétravail sont :

* disposer d'une connexion internet adaptée
* éviter toute utilisation abusive de l’équipement fourni
* entreposer l’équipement non utilisé dans un endroit protégé
* mettre en place des mesures de sécurité adéquates pour la protection de l’information et votre ordinateur portable :
  + pare-feu
  + câble de verrouillage
  + déchiqueteuse de papier
  + coffre-fort
  + logiciel de protection contre les virus à jour
  + écran verrouillé automatiquement après 5 minutes d’inactivité
* suivre toutes les politiques de l'entreprise concernant :
  + la sécurité
  + le cryptage
  + la confidentialité
  + la sauvegarde cryptée des données
  + le code de conduite
  + la durée du travail par jour
* en fin de cession se déconnecter et arrêter ses appareils
* respecter les mesures du moindre accès aux informations sensibles comme celles dans l’organisation
* utiliser de mots de passe forts (à facteurs multiples) et changés régulièrement
* fournir un environnement de travail :
  + avec assez d’espace
  + sécurisé :
    - détecteur de fumée testé
    - trousse de premiers secours
    - numéros d'urgence affichés
  + bureau et chaise appropriés
  + avec une alimentation conforme et testée
  + calme
  + ventilé
  + éclairé
  + isolé des visiteurs et de la famille et
  + sans distractions
* consacrer toute votre attention aux tâches professionnelles pendant les heures de travail
* éviter de télécharger tout logiciel non autorisé
* utiliser la messagerie électronique cryptée
* suivre une formation spécifique sur :
  + la propriété intellectuelle
  + la vie privée
  + les données personnelles
* ne pas oublier que vous êtes entièrement responsable de la sécurité des appareils portables et des actifs informatiques
* vous ne devez pas permettre l'accès non réglementé aux appareils mobiles des membres de votre famille, des personnes proches ou des étrangers résidant accidentellement chez vous