Bureau propre et écran vide

**1. Objet**

**2. Finalité**

**3. Domaine d’application**

**4. Responsabilité**

**5. Documents**

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

**7. Politique bureau propre et écran vide**

Historique

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

**1. Objet**

La politique bureau propre et écran vide a pour objet de sensibiliser le personnel aux exigences relatives à la protection des informations sensibles sur son poste de travail.

**2. Finalité**

La politique bureau propre et écran vide a pour finalité de réduire les risques d'accès non autorisé, de perte et d'endommagement de l’information sur les bureaux, les écrans et dans d'autres endroits accessibles pendant et en dehors des heures normales de travail.

**3. Domaine d’application**

La politique bureau propre et écran vide s’applique à tous les postes de travail dans notre organisation.

**4. Responsabilité**

Le responsable sécurité de l’information (RSI) a l’autorité de l’écriture et de la mise à jour de la politique bureau propre et écran vide. Il est garant de son application. Il a l’appui du directeur et de tous les responsables de département.

**5. Documents**

Protection des matériels

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

A.7.7 Bureau propre et écran vide

Des règles du bureau vide, dégagé des documents papier et des supports de stockage amovibles, et des règles de l'écran vide pour les moyens de traitement de l'information, doivent être définies et appliquées de manière appropriée.

**7. Politique bureau propre et de l’écran vide**

La politique bureau propre et écran vide est communiquées à l’ensemble du personnel et à toutes les parties intéressées concernées.

Les éléments suivants sont pris en compte :

* enfermer les informations commerciales sensibles ou critiques sur papier ou sur des supports de stockage électroniques dans un coffre-fort, une armoire ou une autre forme de mobilier sécurisé lorsqu'elles ne sont pas nécessaires (en fin de journée)
* protéger les terminaux d’utilisateur par des serrures à clé ou d'autres moyens de sécurité lorsqu'ils ne sont pas utilisés ou sans surveillance, cf. le fichier Protection des matériels
* laisser les terminaux d’utilisateur déconnectés ou protégés par un mécanisme de verrouillage de l'écran et du clavier contrôlé par un mécanisme d'authentification de l'utilisateur lorsqu'ils sont sans surveillance. Chaque ordinateur est déverrouillé avec un mot de passe
* configurer tous les ordinateurs et systèmes avec une fonction de temporisation ou de déconnexion automatique
* collecter immédiatement les documents sensibles ou classés en sorties des imprimantes ou des appareils multifonctions. Les imprimantes avec une fonction d’identification par code personnel sont utilisées dans certains locaux par des personnes privilégiées
* stocker en toute sécurité les documents et les supports de stockage amovibles contenant des informations sensibles et, lorsqu'ils ne sont plus nécessaires, les éliminer à l'aide de mécanismes d'élimination
* établir et communiquer des règles et des conseils pour la configuration des fenêtres contextuelles sur les écrans (désactiver les nouvelles fenêtres contextuelles de messagerie, si possible, pendant les présentations, le partage d'écran ou dans un espace public)
* effacer les informations sensibles ou critiques sur les tableaux blancs et autres types d'affichage lorsqu'ils ne sont plus nécessaires

La politique bureau propre et écran vide tient compte :

* de la classification de l’information
* des exigences légales et contractuelles
* des risques associés
* de la culture d’entreprise

Les clés de ces meubles sont entreposées chez le gardien de l’étage.

L’utilisation non autorisée de photocopieurs et autres appareils de reproduction (par exemple les scanners, appareils photo ou téléphones) est interdite.

Les ordinateurs portables sont attachés avec des câbles de sécurité.

Tout utilisateur est tenu de vérifier s'il y a des documents, des pages séparées, des disques, des mémoires portables ou autres objets similaires tombés par inadvertance sous ou derrière les meubles de bureau, dans les vêtements de travail ou personnels et dans d'autres endroits similaires.

Les scanners, télécopieurs, imprimantes sont vérifiés pour des feuilles ou informations restantes dans leur mémoire. Vérifiez particulièrement attentivement les pages non imprimées sur les imprimantes et les télécopieurs et les originaux oubliés et les copies oubliées dans les copieurs.

Lorsqu'il quitte le lieu de travail pour une courte période et en fin de journée, l'utilisateur s'assure que le système est verrouillé et que les personnes non autorisées n'auront pas accès à l'ordinateur, aux documents, aux données, aux outils et à d'autres informations confidentielles.