# Guide
# Sécurité physique

## 1. Accès

L'accès à vos bureaux et à vos archives ne doit être possible que pour les personnes autorisées. Les clés ne doivent pas être transmises à des tiers et il convient de documenter qui possède quelle clé. Les visiteurs et les invités doivent être accompagnés et ne doivent pas pouvoir se déplacer dans les locaux sans être surveillés.

☞ **Liste de contrôle** :

- □ Établir / actualiser le plan des clés
- □ Faire contrôler les portes d'accès et les fenêtres par un spécialiste. Vous trouverez de plus amples informations et une liste de spécialistes sur https://www.sicher-ses.ch/fr?set_language=fr.

## 2. Politique en matière de rangement du bureau (clean desk policy)

Les directives en matières de rangement du bureau définissent l'aspect du poste de travail lorsque les collaboratrices et les collaborateurs quittent le bureau (poste de travail). Il s'agit de garantir que les données sensibles sont conservées en toute sécurité lorsque le poste de travail n'est pas occupé. Il est recommandé de définir par écrit des directives en matière de rangement de bureau comprenant au moins les points suivants :

- Tous les documents contenant des informations sensibles doivent être conservés sous clé (ne pas laisser la clé à l'intérieur !). De tels documents ne doivent donc pas être laissés en évidence, au mur, sur le tableau blanc, sur le flipchart, dans la corbeille à papier, dans les dossiers de signatures, dans les casiers de la poste ou des coursiers, dans l'imprimante, dans l'appareil multifonctions ou dans les vieux papiers.
- Les supports de stockage, tels que les clés USB, les cartes mémoire, les disques durs, et les appareils mobiles, tels que les smartphones et les tablettes, ainsi que les dictaphones, doivent être rangés sous clé.
- Tous les déchets de papier contenant des informations sensibles doivent être éliminés dans le destructeur de documents prévu à cet effet.
- Il ne doit y avoir aucune trace de mot de passe ou de code de coffre-fort, par exemple sur des bouts de papier sous le téléphone, sous le sous-main ou dans le tiroir du haut.
- À la fin de la journée de travail, les ordinateurs doivent être éteints. En cas de courte absence du poste de travail, l'ordinateur doit être verrouillé.
- Toutes les fenêtres doivent être fermées à la fin du travail. En cas de courte absence du poste de travail, il faut fermer les fenêtres qui présentent un risque d'effraction (au rez-de-chaussée).
- A la fin de la journée de travail, le poste de travail doit être rangé ; aucune pile de papier ne doit rester sur le pupitre.

☞ **Liste de contrôle :**

- □ Définir et mettre en œuvre des directives en matière de rangement du bureau pour votre entreprise et vérifier ensuite régulièrement qu'elles soient respectées.

## 3. Post-it, flipcharts et tableaux d'affichage

Il n'y a pas qu'à son propre poste de travail qu'il faut éviter de noter des mots de passe ou des données sensibles sur des post-it, mais aussi sur des tableaux d'affichage ou des flip charts. Celui qui utilise un tableau à feuille est responsable de jeter ensuite les pages sur lesquelles il a écrit ; les données sensibles doivent être détruites dans un destructeur de documents.

☞ **Liste de contrôle :**

- □ Indiquer près du tableau à feuille, que les pages utilisées doivent être immédiatement éliminées.

### 4. Clés USB, supports de données et ordinateur portable

Les clés USB ne sont pas protégées contre les accès non autorisés, il convient donc d'être particulièrement prudent. Si des données sensibles sont stockées sur des clés USB ou d'autres supports de données, elles doivent être cryptées. Cela peut se faire à l'aide d'un logiciel, par exemple **VeraCrypt** ou **BitLocker**, intégré dans les systèmes Windows modernes. Il existe également des supports de données avec un cryptage intégré.

☞ **Liste de contrôle :**

- □ Utilisez des clés USB / supports de données avec cryptage des données.
- □ Contactez votre partenaire informatique pour crypter les données sur le disque dur de votre ordinateur portable.

### 5. Mobilier de bureau verrouillable

Les directives en matières de rangement du bureau

Le mobilier de bureau verrouillable est un élément essentiel des directives en matières de rangement du bureau. Les collaborateurs peuvent ainsi stocker des documents sensibles dans un endroit sûr. Les meubles devraient au moins disposer d'une fermeture à trois points. Un plan de clés devrait également être établi pour les meubles de bureau. Les documents très sensibles, qui devraient en tout cas être conservés à l'abri des effractions et des incendies, doivent être placés dans un coffre-fort (interne ou externe, par exemple dans un coffre-fort d'une banque). Il existe des serrures d'appoint pour les meubles de bureau qui ne sont pas encore verrouillables, faciles à trouver en ligne. Les archives externes conviennent pour stocker des documents en toute sécurité lorsqu'il n'y a pas de place pour les conserver au bureau. Vous trouverez des services d'archivage certifiés dans toute la Suisse sous www.archivsuisse.ch.

☞ **Liste de contrôle :**

- □ Créer / mettre à jour le plan des clés du mobilier de bureau.
- □ Équiper les meubles de bureau de serrures.
- □ Vérifier quels documents devraient être conservés dans un coffre-fort ou un casier fermé à clé.

### 6. Elimination de documents

Dans le domaine de la destruction des données, il convient également de veiller à la sécurité des données. Les dossiers et documents peuvent être découpés et réduits à l'aide d'un destructeur de documents, de sorte que les contenus sensibles ne soient plus lisibles, puis éliminés dans différentes poubelles. Une autre possibilité serait d'externaliser l'élimination sécurisée des documents confidentiels, par exemple en les faisant collecter par des destructeurs de documents professionnels, comme Reisswolf. De cette manière, les documents sont détruits de manière fiable selon des processus certifiés.

Pour le tri des vieux papiers :

- Ce que l'on ne montrerait pas à un visiteur lors d'une journée portes ouvertes ne devrait pas non plus être jeté dans le vieux papier.
- Les documents imprimés dans l'entreprise ne doivent pas être jetés avec le vieux papier normal.
- Tous les documents portant une adresse ne doivent pas être jetés dans le vieux papier.

Idéalement, la séparation entre « confidentiel » et « inoffensif » devrait avoir lieu le plus tôt possible - cela permet de réduire le travail de tri.

☞ **Liste de contrôle :**

- □ Apposer une note près du vieux papier indiquant quels documents doivent être détruits.

## 7. Documents confidentiels

Les documents confidentiels qui contiennent des données sur les clients, les collaborateurs ou le développement doivent être marqués en conséquence. Le marquage doit permettre d'identifier facilement le groupe de classification des informations auquel appartiennent les documents.

Classification des informations :

- **Public** : Les données sont accessibles à tous, y compris aux personnes extérieures à l'entreprise. La divulgation des informations n'a pas de conséquences négatives. Par exemple : brochures, publications
- **Interne** : Les données ne sont accessibles qu'aux collaborateurs de l'entreprise. La divulgation des informations peut entraîner un préjudice faible à moyen. Par exemples : Listes de prix, descriptions de processus, organigrammes.
- **Confidentiel** : Les données ne sont accessibles qu'à un certain nombre de collaborateurs. La divulgation des informations peut causer un dommage important. Par exemple : données sur le personnel, listes de clients, calculs.
- **Strictement confidentiel** : Les données ne sont accessibles qu'à un groupe de personnes strictement défini. La divulgation de ces données peut mettre en péril l'existence de l'entreprise. Par exemple : données relatives au développement, stratégie de l'entreprise

Vous trouverez des lignes directrices pour la classification des informations selon la norme ISO/IEC 270001 sous : https://www.sec4you.com/klassifizierung-iso-27001/

**☞ Liste de contrôle :**

- □ Déterminer quelles classifications doivent être utilisées dans votre entreprise.
- □ Créer des modèles Word/Excel dans lesquels le statut de confidentialité doit être indiqué.

## 8. Conversations (téléphoniques) confidentielles

Il est de la responsabilité de l'employeur de protéger la vie privée des collaborateurs et des clients. Veillez à ce que les conversations confidentielles puissent se dérouler dans un espace protégé, sans que des informations ne soient divulguées à l'extérieur.

On trouve en ligne des boîtes téléphoniques avec porte vitrée qui peuvent être installées dans un bureau.