Baloise
SCOUTS
DIGITAUX

Conseils et astuces pour travailler au bureau à domicile

Nous vous montrons le chemin à travers la jungle digitale.

www.baloise.com/digitale-pfadfinder

Baloise
Group

Des conditions de travail optimales au bureau à domicile

De plus en plus d'employés travaillent en dehors du bureau. Mais y-a-t'il un environnement de travail approprié, une sécurité informatique suffisante et une protection des données dans le bureau à domicile? Avec cette brochure, nous souhaitons vous donner des conseils et des astuces pour le travail à domicile.

→ Créer de bonnes conditions pour travailler au bureau à domicile. Une bonne infrastructure telle que des connexions internet rapides, divers outils de communication et de gestion de projet ou peut-être un grand écran soutiendra le travail.

→ Un défi majeur est la difficulté de communication lorsque l'on travaille dans des équipes réparties localement. Utiliser des moyens de communication avec lesquels on peut discuter ensemble en ligne via la vidéoconférence, le chat et les outils de projet. Une description des applications utiles pour la collaboration se trouve sur le site web «be-digital» de la Chambre de commerce de Bâle: www.hkbb.ch/de/be-digital_hilfreiche_Anwendungen_fuer_die_Zusammenarbeit.php

→ Mettre en place un groupe de travail commun et organiser des réunions hebdomadaires sur le statut de l'équipe.

→ Introduire une rétrospective lors des réunions d'équipe: Qu'est-ce qui s'est bien passé, qu'est-ce qu'on garde? Comment améliorer notre collaboration et nos processus à l'avenir?

→ Vous pouvez vous réunir tous les matins ou au moins deux fois par semaine dans une réunion vidéo d'environ 15 minutes. Tenez-vous informés les uns les autres:

→ Quel est l'état d'avancement des travaux en cours ou des projets en cours? Comment pouvons-nous nous soutenir mutuellement? L'expérience montre que les réunions sont plus efficaces lorsque la caméra est allumée. Cela apporte de la personnalité dans la coopération. Toute personne qui ne parle pas doit couper son microphone. Cela permet d'éviter les bruits de fond gênants.

→ Maintenez un contact régulier avec vos employés et favorisez l'échange d'informations entre eux. La communication informelle est également importante pour votre bien-être. Prenez sans cesse les réactions de vos employés. Par exemple, vous pouvez organiser des tournées de café quotidiennes par vidéoconférence.

→ Le travail à domicile présente également de nombreux avantages. Les activités qui exigent un haut niveau de concentration et de créativité sont les mieux adaptées à cette fin. Il s'agit notamment de préparer une présentation, de préparer une offre complexe ou de documenter les processus commerciaux. Les horaires de travail peuvent être librement aménagés tout au long de la journée.

→ La journée de travail doit être bien organisée et structurée. Vous gardez donc la vue d'ensemble.

→ Il est important de respecter les temps de travail et de pause: Travailler pendant les heures de travail, se lever pendant les pauses. Planifier volontairement des pauses. Il est conseillé de noter les heures travaillées.

→ Les pauses pour faire de l'exercice sont importantes pour un travail sain: Levez-vous et marchez, faites des étirements et changez de position assise de temps en temps. Faites une promenade ou un jogging pendant le déjeuner ou après le travail. Il existe également un large éventail de vidéos de formation en ligne, dont certaines peuvent être utilisées gratuitement.

→ Les règles minimales en matière de contrat de travail pour les bureaux à domicile peuvent être consultées sur le site Internet du Secrétariat d'Etat à l'économie SECO:
https://www.seco.admin.ch/seco/de/home/Publikationen_Dienstleistungen/Publikationen_und_Formulare/Arbeit/Arbeitsbedingungen/Broschuren/homeoffice.html
et sur le site de l'Association des employeurs de Bâle:
https://www.arbeitgeberbasel.ch/dienstleistungen/recht/coronavirus-covid19/homeoffice/

Sécurité informatique

→ Il se peut qu'en tant qu'entreprise, vous ayez besoin d'une utilisation beaucoup plus importante des bandes passantes, des services informatiques et de l'infrastructure utilisés. Vérifiez exactement quels sont les domaines et les processus prioritaires afin que l'ensemble de l'infrastructure continue de bien fonctionner. Augmenter les capacités selon les besoins.

→ Sauvegardez vos données et faites des sauvegardes. Ce n'est pas seulement en cas de cyber-attaque que des données sensibles telles que des informations sur les clients ou des transactions peuvent être perdues. D'autres influences externes, telles que les incendies ou les dégâts des eaux, peuvent également entraîner des pertes de données. Vous devez donc faire des sauvegardes régulières.

→ Installez à temps les mises à jour régulières de service et de sécurité pour votre système d'exploitation et vos programmes.

→ Un mot de passe fort doit être utilisé pour chaque service et un second facteur d'identification, par exemple des jetons RSA ou un code à usage unique par SMS.

- La sécurité de l'information est la tâche et le défi de chaque employé. Néanmoins, vous devez nommer une personne responsable de la sécurité de l'information dans votre entreprise et un adjoint.

- Les employés doivent utiliser l'équipement fourni par l'entreprise si possible. Les logiciels antivirus et les pare-feu s'appliquent également au travail à domicile.

- Sensibilisez vos employés aux dangers et aux risques du réseau. Les points d'accès publics aux réseaux locaux sans fil (WLAN) sont à éviter, les connexions VPN sont sûres.

- Veillez à ce que les exigences en matière de sécurité et de protection des données soient respectées pour les moyens de communication utilisés. Utilisez des services cryptés dans la mesure du possible. Formez vos employés afin qu'ils puissent respecter les mesures de sécurité. Souligner que seuls les outils internes à l'entreprise doivent être utilisés.

- La sécurité informatique et la protection des données s'appliquent également au travail dans les bureaux à domicile. Les informations internes confidentielles de l'entreprise ou les données des clients ne doivent pas être consultées par des personnes non autorisées. Une salle de travail séparée est idéale. Les données sensibles, par exemple, ne doivent pas être traitées sur la terrasse ou dans un café public.

- Le Centre national pour la cybersécurité (NCSC) a constaté que les pirates informatiques exploitent de plus en plus de failles de sécurité pour accéder aux réseaux d'entreprises en utilisant diverses méthodes. Ils peuvent causer de grands dégâts. Protégez votre entreprise par des mesures appropriées!

- Le soutien de l'État et d'autres mesures visant à réduire les cyberrisques en raison de la situation actuelle des menaces peuvent être consultés sur le site de la Centrale fédérale d'enregistrement et d'analyse pour la sûreté de l'information MELANI www.melani.admin.ch

Les règles d'or pour un mot de passe sécurisé

1. Les mots de passe doivent comporter au moins 8 caractères contenant des majuscules et minuscules, des chiffres et des caractères spéciaux.

2. Les mots de passe doivent être changés au moins tous les 3 mois

3. Les mots de passe ne doivent pas être simples à deviner, en particulier ils ne doivent pas comporter de référence reconnaissable au propriétaire du mot de passe, par exemple pas de noms de personnes, d'animaux de compagnie, anniversaire de personnes proches … En outres les mots de passe provenant de dictionnaire ne doivent pas être utilisés

4. Un nouveau mot de passe ne doit pas faire référence à un mot de passe qui a été utilisé récemment.

5. Le mot de passe par défaut doit immédiatement être changer lors de la première mise en service

6. les mots de passe ne doivent jamais être écrits. Si vous avez oublié votre mot de passe, vous pouvez contacter le service d'assistance.

7. Tous les mots de passe doivent rester personnels et strictement confidentiels et ne peut être transmise à d'autres personnes.

Cette brochure a été réalisée par les Baloise Digital Scouts, une initiative des collaborateurs du groupe Baloise. De plus amples informations et le Cyber Security Guide sont disponibles à l'adresse suivante:
www.baloise.com/digitale-pfadfinder

Baloise Group
Aeschengraben 21
CH-4002 Basel
pfadfinder@baloise.com

www.baloise.com

11250-01f 6.20 50