Vos Déplacements Pros en Toute Sérénité : Le Guide Ultime pour les Nouveaux Collaborateurs

Sous-titre : *Équipement, sécurité et bonnes pratiques : on vous explique tout !*

Chers collègues, bienvenue chez WELCOME ! 🌟

Vous venez de rejoindre notre entreprise et vous vous apprêtez à rencontrer des clients en présentiel ou en télétravail ? Pas de panique : WELCOME met à votre disposition **tout l'équipement nécessaire** pour travailler en sécurité, où que vous soyez. Pas besoin de configurer un VPN ou d'installer des logiciels : tout est déjà prêt ! Voici nos conseils pour transformer vos déplacements en succès.

---

1. Votre Kit Pro : Ce Que WELCOME Vous Fournit

Avant même votre premier départ, vous recevrez :

- 💻 **Un ordinateur portable sécurisé** : Préconfiguré avec le VPN WELCOME, un antivirus et les outils métiers (CRM, messagerie, etc.).
- 📱 **Un téléphone professionnel** : Pour rester joignable sans partager votre numéro personnel.
- 🔑 **Une clé USB chiffrée** : Pour transférer des fichiers en toute sécurité (à utiliser uniquement en cas de nécessité !).
- ⚡ **Un chargeur universel** : Compatible avec toutes les prises, idéal pour les déplacements à l'étranger. Ne supporte Uniquement le chargement, pas le transfert de données

👉 *Vous avez déjà tout sous la main ? Parfait ! Contactez le service IT si un équipement manque ou semble défectueux.*

---

2. Le VPN WELCOME : Votre Bouclier Numérique (Déjà Actif !)

Pas de configuration complexe : le VPN est **activé par défaut** dès votre première connexion. Son rôle ? **Protéger vos échanges** comme si vous étiez au siège.

- **À faire** :
    - Laissez le VPN **toujours allumé** pendant vos déplacements.
    - Utilisez-le pour accéder aux dossiers clients, à la messagerie interne ou aux outils collaboratifs.
- **À éviter** :
    - Désactiver le VPN pour "gagner en vitesse" (la sécurité prime !).
    - Partager vos identifiants : chaque compte est personnel et tracé.

💡 *Le saviez-vous ?* Notre VPN utilise un chiffrement militaire (AES-256) pour rendre vos données illisibles en cas de piratage.

---

3. Clés USB et Stockage : La Prudence est de Mise

Les clés USB, pratiques mais risquées, doivent être utilisées avec parcimonie :

- **Autorisées uniquement** :
    - Pour transférer des fichiers **non sensibles** (présentations clients sans données stratégiques).
    - Avec la clé USB chiffrée fournie par WELCOME.
- **Strictement interdites** :
    - Utiliser des clés USB personnelles (risque de virus).
    - Stocker des mots de passe, des contrats confidentiels ou des données clients sensibles.

👉 *Alternative sécurisée :* Privilégiez le cloud WELCOME (*SecureCloud*), accessible via le VPN, pour partager ou sauvegarder vos fichiers.

---

4. Téléphone Pro et Chargeurs : Restez Connectés Sans Risque

- **Votre téléphone WELCOME** :
    - Ne l'utilisez que pour le travail : pas d'applications personnelles (réseaux sociaux, jeux).
    - Activez le verrouillage automatique après 1 minute d'inactivité.
- **Chargeurs et bornes publiques** :
    - Évitez les ports USB publics (gares, aéroports) : ils peuvent installer des logiciels espions.
    - Utilisez le chargeur universel WELCOME ou une prise électrique classique.

🚨 *En cas de perte ou vol* : Contactez immédiatement le service IT pour bloquer l'appareil à distance.

---

5. Réseaux Wi-Fi : Les Bonnes Pratiques

Même avec un VPN, mieux vaut éviter les réseaux douteux :

- **Priorité à la 4G/5G** : Utilisez le partage de connexion de votre téléphone WELCOME.
- **En Wi-Fi public** (hôtel, café) :
    - Vérifiez le nom exact du réseau avec le personnel (ex. : "HôtelXYZ_Guest").
    - Ne consultez jamais vos comptes perso (banque, réseaux sociaux) sur ces réseaux.

---

6. Et N'Oubliez Pas…

- **Les mises à jour** : L'ordinateur et le téléphone se mettent à jour automatiquement. Ne reportez jamais ces mises à jour !
- **Les gestes physiques** :
    - Verrouillez toujours votre écran en quittant votre poste.
    - Transportez vos équipements dans une sacoche discrète, sans logo WELCOME visible.

- Ne discutez pas de sujets sensibles dans des espaces ouverts ou en présence d'inconnus.
- Ne laissez aucun document ou élément confidentiel à la vue des autres, que ce soit sur un bureau ou un écran
- Adaptez votre comportement aux règles de sécurité du client et respectez ses protocoles internes.

- **La charte IT** : Relisez-la sur l'intranet pour éviter les malentendus.

FAQ des Nouveaux Collaborateurs

- **Q : Puis-je utiliser mon ordinateur personnel pour le travail ?**
  R : Non. Seul le matériel fourni par WELCOME est autorisé, pour des raisons de sécurité.
- **Q : Que faire si ma clé USB est perdue ?**
  R : Signalez-le immédiatement à IT. Grâce au chiffrement, les données seront illisibles, mais mieux vaut bloquer l'accès.
- **Q : Puis-je charger mon téléphone perso avec le chargeur WELCOME ?**
  R : Oui, mais évitez de le connecter à votre ordinateur professionnel.

Conclusion : Votre Sécurité, Notre Priorité 🛡️

Chez WELCOME, nous croyons que la mobilité ne doit pas compromettre la sécurité. En suivant ces conseils, vous protégerez non seulement nos données, mais aussi votre réputation et celle de nos clients.

Besoin d'aide ?

- Service IT : **support-it@welcome.com** ou poste #4350.
- Urgence (vol/perte) : **24/7 via le numéro de téléphone d'urgence**

Bienvenue à bord, et bonnes aventures professionnelles !

Écrit par l'équipe Cybersécurité WELCOME, avec le sourire 😊.