cogeco | AFFAIRES

Directives de sécurité pour la Téléphonie hébergée

Découvrez comment optimiser la sécurité de votre système téléphonique avancé. Protégez votre entreprise contre les imprudences et aidez à prévenir les accès non autorisés en suivant ces directives.

Restriction téléphonique

- Si vous ne faites jamais d'appels internationaux et que vous ouhaitez éviter l'utilisation non autorisée des appels internationaux, veuillez nous appeler pour bloquer cette fonction.
- Cogeco offre des restrictions distinctes pour différents types d'appels, tels que le 011 (international), le 1 900 (appels surtaxés), le 1010 (appels CIC), etc.
- Veuillez vous assurer que cette démarche est effectuée pour chaque ligne téléphonique partagée, car elles auront toutes des restrictions distinctes.

Modification de l'équipement ou de la configuration

- Ne déplacez pas les appareils téléphoniques, ne modifiez pas leur configuration physique et ne branchez pas les appareils directement sur un modem sans contacter Cogeco.

Gestion des utilisateurs et comptes

- Veuillez nous contacter pour révoquer les privilèges d'accès des sièges et utilisateurs non utilisés ou des utilisateurs licenciés.

Sécurité du poste de travail
(pour les utilisateurs de Max UC sur PC)

- Verrouillez toujours votre poste/ordinateur pour empêcher tout accès ou utilisation non autorisée du logiciel.
- Assurez-vous que vous utilisez toujours la dernière mise à jour de la version de sécurité et de la protection antivirus sur votre poste de travail individuel.

Portail administrateur

- Les mots de passe de votre portail d'administration et de Max UC doivent être suffisamment complexes. Veuillez vous abstenir d'utiliser des mots de passe simples (par exemple, 0000).
- Veillez à ne pas partager vos mots de passe à l'extérieur de votre entreprise.

Systèmes de messagerie vocale

- Les mots de passe ou les NIP doivent comporter un minimum de 6 caractères. Il est préférable d'utiliser le nombre maximal de caractères.
- Les mots de passe ne doivent pas être faciles à deviner, et ne doivent jamais être affichés ou partagés. N'utilisez pas de combinaisons de chiffres telles que l'emplacement du téléphone ou le numéro de téléphone à 7 chiffres. Il est recommandé d'utiliser, si possible, des logiciels qui testent la sécurité des mots de passe.
- Les mots de passe ne devraient jamais correspondre à l'emplacement de l'appareil téléphonique lorsqu'il est attribué à un nouvel utilisateur.
- Invitez les utilisateurs à modifier le NIP de leur messagerie vocale à intervalles de 30 jours à 60 jours.

Sécurité des appareils mobiles
(pour les utilisateurs mobiles de Max UC)

- Si vous avez des employés qui utilisent Max UC sur leurs téléphones mobiles, veuillez vous assurer que leurs appareils téléphoniques ont un NIP, l'identfication faciale ou par empreinte digitale pour empêcher l'utilisation non autorisée du logiciel.

Pour plus d'information

Si vous avez des questions sur les risques de fraude téléphonique, nos experts sont là pour vous aider et répondre à toutes vos questions au **1 855 494-5853**.