COGECO | AFFAIRES

Directives de sécurité pour la Téléphonie gérée Cogeco

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

- Cogeco offre des restrictions distinctes pour différents types d'appels, tels que le 011 (international), le 1900 (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.
- Pour votre protection, les appels interurbains internationaux sont désactivés par défaut. Contactez-nous si vous souhaitez les activer.

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'identification faciale ou par empreinte digitale pour empêcher l'utilisation non autorisée du logiciel.

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.

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.

Item 11346 07/24

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.

cogeco | BUSINESS

Cogeco Managed Telephony Security Guidelines

Learn how to maximize the security of our advanced phone service. Protect your business from negligent mistakes and help prevent unauthorized access by following these guidelines.

Toll restriction

- Cogeco offers separate restrictions for different types of calls, such as 011 (international), 1-900 (premium calling), 1010 (CIC calling), etc.
- Please ensure this is done for each common phone as they will all have separate restrictions
- For your protection, international long distance is disabled by default. Please contact us to enable it if needed.

Mobile device security (For Max UC mobile users)

- If you have employees using Max UC on their mobile phones, please make sure their phones have PINs, face IDs or fingerprint IDs to prevent unauthorized use of software.

User/account management

- Please contact us to revoke access privileges for unused seats/users or terminated employees.

Workstation security (for Max UC desktop users)

- Always lock your station/computer to prevent unauthorized access or use of the software.
- Make sure you are always running the latest security version and virus protection on your individual desktop.

Comm portal

- Your admin portal and Max UC passwords should be complex. Please refrain from using simple passwords (for example, 0000).
- Make sure you do not share your passwords outside of your organization.

Voicemail systems

- Passwords or PINs should be a minimum of 6 characters. It is best to use the maximum number of characters.
- Passwords should not be easy to guess, and should never be posted or shared. Don't use common number schemes such as the location of the telephone or the 7-digit telephone number. Software packages that test for common passwords should be used where possible.
- Passwords should never be set to the location of the telephone when assigned to a new subscriber.
- Invite users to change their voicemail PINs at 30 or 60 day intervals.

Tampering with the equipment or setup

- Do not move the phones, change the physical setup or plug the phones directly into a modem without contacting Cogeco.

Item 11346 07/24

For more information

If you have any questions about toll fraud, our experts are here to assist you and answer any questions that you may have. We can be reached at 1-866-264-3262.