10 règles d'or pour la cybersécurité

 Modèle

# Autorité et révision

## Contrôle et révision des documents

|  |  |
| --- | --- |
| **Vérification des documents**  |  |
| Auteur  |  |
| Propriétaire |  |
| Date de création |  |
| Dernière révision par  |  |
| Date de la dernière révision |  |

.

## Gestion des versions

|  |  |  |  |
| --- | --- | --- | --- |
| **Version**  | **Date d'approbation** | **Approuvé par**  | **Description du changement** |
| 1.0 |  |  |  |

# 10 règles d'or pour la cybersécurité

|  |  |
| --- | --- |
|  | **Protégez vos comptes avec une authentification forte !****Utilisez toujours l'authentification multifactorielle (MFA) dans la mesure du possible !*** Les mots de passe longs sont plus efficaces car ils sont plus difficiles à déchiffrer pour les cybercriminels, étant donné les nombreuses possibilités offertes par le nombre de caractères.
* Les mots de passe forts comportent au **moins 14 caractères, ne sont pas faciles à deviner et contiennent : des majuscules, des minuscules, des caractères numériques, des caractères spéciaux (&,$,%, !,=,+...).**
 |
|  | Utilisez des mots de passe différents pour les comptes professionnels et personnels |
|  | Stockez toutes vos données dans un système où des sauvegardes sont effectuées régulièrement et de manière centralisée. |
|  | Exécutez les mises à jour de sécurité sur tous vos appareils dès qu'elles sont disponibles. |
|  | Ne laissez jamais d'informations physiques (par exemple des documents papiers) ou d'appareils sans surveillance sur votre bureau. |
|  | Évitez les réseaux Wi-Fi publics et utilisez le réseau privé virtuel (VPN) de l'entreprise. |
|  | **Évitez le phishing en vous posant les questions suivantes** :* L'expéditeur est-il quelqu'un que je connais ?
* Est-ce que je m'attendais à un message sur le sujet mentionné ?
* Le message demande-t-il des informations telles qu'un nom d'utilisateur, un mot de passe ou un numéro de compte bancaire ?
* Est-ce urgent ?
* Où mène le lien ? (Placez votre curseur sur le lien sans cliquer.)
* Le message contient-il un code QR ?
* S'adresse-t-on à moi personnellement ?
* Le message contient-il des fautes d’orthographe ?
* Le message se trouve-t-il dans le dossier Spam / Junkmail ?
* Quelqu'un essaie-t-il de susciter ma curiosité ?
* Est-ce qu’un paiement est demandé ?

**Comment répondre à un courriel de phishing ?*** Ne répondez pas à ces messages, n'ouvrez pas les pièces jointes et ne cliquez pas sur les liens.
* Ne communiquez jamais de coordonnées bancaires demandées par SMS ou par e-mail.
* Signalez la tentative d'hameçonnage au **[service informatique/fournisseur]** et supprimez l'e-mail/le SMS.
 |
|  | Respectez les mesures suivantes lorsque vous manipulez des informations internes ou confidentielles :* Verrouillez votre ordinateur si vous le laissez sans surveillance.
* Ne laissez pas d'ordinateurs ou de documents sans surveillance sur les bureaux en dehors des heures de travail.
* Ne laissez pas de documents sans surveillance dans les imprimantes.
* Surveillez toujours votre entourage lorsque vous consultez ou discutez des informations confidentielles dans des lieux publics. Essayez de vous isoler autant que possible pour éviter que quelqu'un n'entende une conversation.
 |
|  | N'utilisez que les sites web et les plateformes officielles pour télécharger des applications et des logiciels. Le téléchargement de logiciels est à éviter. Les logiciels sont installés par **le service informatique ou le fournisseur.** |
| Marketing outline | Signalez tous les incidents de sécurité de l'information à votre service informatique/fournisseur. Contactez toujours **[le service informatique/fournisseur]** dans les cas suivants :* si vous avez des questions ou des commentaires sur ce document ;
* si vous constatez quoi que ce soit de contraire au présent document ;
* un incident suspecté ou confirmé se produit.

Coordonnées de contact : **[Numéro de téléphone du département informatique/fournisseur] / [Courriel du département informatique/fournisseur].** |