MOTS DE PASSE UTILISATEUR IDENTIFICATION, UTILISATION ET PROCÉDURES RELATIVES À SA PROTECTION À PROPOS DES PRINCIPES RÈGLEMENTS

KVKK_Y7 VERSION 1.00

1. INTRODUCTION, OBJECTIFS ET DÉFINITIONS

1.1. Le présent règlement définit les procédures applicables et fournit des recommandations aux utilisateurs concernant l'utilisation et/ou la protection des mots de passe des utilisateurs définis/à définir en relation avec tous les types de systèmes d'information et de communication utilisés au sein de la Société.

2. PRINCIPES POUR DÉFINIR UN MOT DE PASSE ROBUSTE

2.1. L'entreprise attend des utilisateurs qu'ils assurent une protection efficace de leurs mots de passe en définissant des mots de passe robustes, respectant les critères suivants : 2.1.1. Le mot de passe doit comporter au moins 8 caractères.

2.1.2. Le mot de passe doit contenir au moins trois des éléments suivants :

(JE) Caractères numériques (0-9)

(II) Lettres majuscules (AZ)

(III) Lettres minuscules (peu nombreuses)

(IV) Caractères spéciaux (?, !, @, #, %, etc.)

2.1.3. Le mot de passe ne doit contenir aucun des éléments suivants :

(I) Un mot tiré d'un dictionnaire (de n'importe quelle langue), de l'argot ou une abréviation générale.

(II) Le nom d'une personne ou d'un lieu.

(III) Une date facilement devinable, telle que l'anniversaire du conjoint/partenaire de l'utilisateur.

(IV) Informations connues pour être liées à l'utilisateur, telles que la plaque d'immatriculation du véhicule de l'utilisateur, le numéro d'identité de la République turque et le numéro de carte d'accès.

(V) Le nom d'utilisateur du compte doit être identique ou similaire à (y compris les noms d'utilisateur inversés ou mal orthographiés)

(VI) Tous les mots de passe, informations, etc. donnés à titre d'exemples sur le site Web de l'entreprise ou dans le présent règlement.

2.1.4. Le nouveau mot de passe ne peut pas être le même que l'un des six derniers mots de passe utilisés.

3. PRINCIPES À SUIVRE POUR LA PROTECTION DES MOTS DE PASSE

3.1. Les utilisateurs doivent choisir un mot de passe mémorable, éviter de taper des mots de passe et, en aucun cas, ne doivent laisser leurs mots de passe dans un endroit où d'autres peuvent facilement y accéder.

3.2. Les utilisateurs ne doivent divulguer leur mot de passe à personne. L'entreprise ne demandera jamais le mot de passe d'un utilisateur. Seul l'utilisateur lui-même a besoin de le connaître.

Si un utilisateur reçoit un courriel, un message, etc., contenant une telle demande, cette communication doit être considérée comme une tentative de fraude électronique, et le responsable informatique doit en être immédiatement informé sans répondre.

3.3. Si un utilisateur découvre que son mot de passe a été divulgué accidentellement ou autrement, il doit le changer immédiatement et en informer rapidement le responsable informatique.

3.4. Les utilisateurs doivent veiller à ce que personne ne puisse voir leur écran lorsqu'ils saisissent leur mot de passe de connexion et ne doivent pas positionner leur écran de manière à ce que quiconque, y compris leurs collègues, puisse les voir saisir leur mot de passe. Les écrans doivent également être placés dans les bureaux de façon à ne pas être visibles de l'extérieur du bâtiment.

3.5. Les utilisateurs ne doivent pas saisir leurs mots de passe sur un site web à moins d'être absolument certains qu'il s'agit du site officiel de communication et d'information de l'entreprise. Le meilleur moyen de s'en assurer est d'ajouter soi-même les sites à ses favoris.

Cela implique de fournir vos propres URL ou d'y accéder via les URL que vous avez saisies. Évitez d'utiliser des liens, notamment ceux contenus dans des courriels se prétendant légitimes.

4. CHANGER LES MOTS DE PASSE

4.1. Il est essentiel que les utilisateurs modifient régulièrement leur mot de passe. Le directeur général adjoint peut fixer la fréquence de modification des mots de passe entre 30 jours et un an, en fonction des rôles et responsabilités des titulaires de compte autorisés par la société.

4.2. Vous pouvez modifier votre mot de passe en vous connectant aux ordinateurs enregistrés dans l'inventaire de l'entreprise et en utilisant le lien suivant : http://www.kardelenboya.com.tr/

4.3. La réutilisation des anciens mots de passe est interdite. Il s'agit d'une bonne pratique, applicable également aux systèmes externes à l'entreprise.

4.4. Les utilisateurs dont les mots de passe ne sont pas conformes aux dispositions du présent règlement seront immédiatement tenus de les modifier.

4.5. Les utilisateurs devant modifier leur mot de passe seront contactés par un employé de la société par courriel, par téléphone ou en personne. Ils pourront ensuite procéder à la modification de leur mot de passe auprès de la société. Il ne doit révéler cela à personne, pas même à son personnel.

5. MOTS DE PASSE À UTILISER POUR LES SYSTÈMES EXTERNES

5.1. Il est recommandé d'appliquer les meilleures pratiques d'utilisation décrites dans le présent règlement lorsque vous utilisez d'autres systèmes en dehors de la Société.

5.2. Évitez d'utiliser votre nom d'utilisateur et votre mot de passe existants au sein de la Société pour créer des comptes sur des sites Web ou d'autres ressources Internet.