TP SYNTHESE

Identifier les points clés de la charte informatique.

1- CADRE DU TÉLÉTRAVAIL
2 - MODALITÉS DE MISE EN OEUVRE
3 – MOYENS MIS À DISPOSITION ET TRAITEMENT DE L'INFORMATION
4 – EXERCICE DU TÉLÉTRAVAIL

Identifier les usages personnels et professionnels

Usage Personnel :

- La charte dit que le télétravail est un choix personnel, ce qui signifie que c'est à chaque personne de décider si elle veut travailler à la maison (Section 1-3).

- Si quelqu'un veut arrêter de travailler à la maison, il peut le faire quand il le souhaite (Section 1-3).
- Il est important que l'endroit où vous travaillez chez vous soit adapté et confortable (Section 4-1)

Identifier les usages personnels et professionnels

Usage Professionnel :

- La charte insiste sur le respect de la vie privée pendant le travail à la maison, disant que cela doit être séparé du personnel (Section 2-1).
- Les objectifs de travail et les responsabilités sont décidés par le responsable, montrant que le travail à la maison a des attentes professionnelles (Section 2-4).
- Les ordinateurs fournis par l'entreprise sont réservés à un usage professionnel (Section 3-1).
- Les règles de confidentialité et de sécurité informatique doivent être respectées, montrant que l'utilisation doit être sécurisée et professionnelle (Section 3-4)

Quelle politique appliqueriez-vous dans la charte informatique en ce qui concerne les fichiers en provenance d'internet.

Responsabilité de l'Utilisateur :

- Insister sur la responsabilité individuelle des utilisateurs pour vérifier la légitimité des fichiers téléchargés et signaler tout comportement suspect

Filtrage des Fichiers :

- Utiliser des outils de filtrage pour analyser et bloquer les fichiers potentiellement malveillants provenant d'internet.

Types de Fichiers Autorisés :

- Limiter les types de fichiers autorisés à être téléchargés depuis internet à ceux nécessaires à des fins professionnelles

Procédures en cas d'incident :

- Établir des procédures claires à suivre en cas de téléchargement accidentel de fichiers malveillants, y compris le signalement immédiat à l'équipe de sécurité informatique

Indiquez comment peut-il intervenir sur les postes de travail pour contrôler l'utilisation des supports USB.

Pour empêcher l'accès aux ports USB pour les utilisateurs sur les comptes administrateurs sous Windows, on peut configurer une Politique de Groupe (GPO) pour restreindre cette fonctionnalité.

Expliquez quelle précaution supplémentaire il doit prendre pour être certain que la configuration réalisée précédemment soit pérenne.

En plus du contrôle des supports USB, il doit aussi faire des sauvegardes régulières du système et des configurations. ce qui permet de revenir à une configurations antérieur en cas de problème

Indiquez quelle application native sous windows permet d’avoir une version récente du système d’exploitation

Windows Update est l'application native sous Windows qui permet d'avoir une version récente du système d'exploitation en installant les mises à jour, tandis que le Centre de sécurité Windows Defender contribue à la sécurité du système, y compris la protection contre les logiciels malveillants

Démontrez que celle-ci peut également agir sur les failles de sécurité.

Les mises à jour régulières du système d'exploitation sont essentielles pour gérer les failles de sécurité. En effectuant ces mises à jour, le système obtient rapidement les correctifs de sécurité nécessaires dès leur disponibilité, renforçant efficacement la protection contre les vulnérabilités.

Précisez quel outil supplémentaire peut être installé sur un poste de travail pour garantir sa sécurité.

Pour augmenter la sécurité des postes on peut utiliser des logiciel anti virus tel que McAfee , Avast, panda. ils peuvent détecter et eliminer les malwares, les virus et autres menaces potentielles

Guide des bonnes pratiques afin d'encadrer les usages de ses étudiants et ainsi de les responsabiliser

Complexité des Mots de Passe :

- Les mots de passe doivent être complexes, comprenant une combinaison de lettres majuscules et minuscules, de chiffres et de caractères spéciaux.

Longueur des Mots de Passe :

- Les mots de passe doivent avoir une longueur minimale recommandée de 12 caractères pour assurer une meilleure sécurité.

Éviter les Informations Personnelles :

- Les étudiants doivent éviter d'inclure des informations personnelles telles que leur nom, date de naissance, ou d'autres données facilement accessibles.

Renouvellement Régulier :

- Il est recommandé de renouveler les mots de passe à intervalles réguliers pour réduire les risques liés à une éventuelle compromission.

Guide des bonnes pratiques afin d'encadrer les usages de ses étudiants et ainsi de les responsabiliser

Stockage Sécurisé :

- Il est fortement déconseillé de stocker les mots de passe de manière non sécurisée, comme sur des post-its ou dans des fichiers facilement accessibles. mais plutôt d'utiliser un stockage de mot de passe en ligne comme keypass certifié avec lanssi

Authentification à Deux Facteurs (2FA) :

- Lorsque possible, encouragez l'activation de l'authentification à deux facteurs pour une couche supplémentaire de sécurité.

Précisez les recommandations à suivre pour la gestion des mots de passe durant les deux années de BTS

Utiliser keypass comme gestionnaire de mots de passe pour les deux années de bts est fortement conseillé

Méthode 1 passphrase

Composition de Mots Aléatoires :

- Dans cette méthode, le mot de passe par passphrase est créé en combinant des éléments de manière aléatoire. Cela peut inclure des mots choisis au hasard, des chiffres et des caractères spéciaux. L'objectif est de former une phrase complexe et unique, rendant ainsi le mot de passe difficile à deviner.
- Par exemple, une passphrase générée de manière aléatoire pourrait ressembler à ceci : "B@nane42#Rouge!"

Méthode 2 passphrase

Utilisation de Phrases Complexes :

- Cette méthode implique la création d'un mot de passe en utilisant une phrase complexe ou une série de mots significatifs. La complexité est ajoutée en incluant des variations de majuscules, de minuscules et l'ajout de caractères spéciaux. L'idée est de former une passphrase mémorable mais difficile à déchiffrer.
- Par exemple, une passphrase basée sur une phrase complexe pourrait être : "Sauter!7Montagnes#Réussir."

Indiquez quelles manipulations ne sont pas souhaitables et expliquez pourquoi.

Enregistrement Automatique des Mots de Passe

connexion à partir d'Appareils Non Sécurisés

Utilisation d'Identifiants Faibles

Expliquez le rôles des différents stratégies de sécurité locales

Le rôle des différentes stratégies est de pouvoir réglementer la politique de mot de passe