EPREUVE THEORIQUE D'INFORMATIQUE

Nom et prénom ……Classe……..

Compétences : utiliser les périphériques et pratiquer la sécurité informatique.

PARTIE A : UTILISATION DES PERIPHERIQUES /10 POINTS

Pour s'adapter au nouvel environnement du système d'enseignement par digitalisation, votre enseignant d'informatique pose sur son bureau les équipements suivants : une souris, un clavier ; une unité centrale, un écran, une imprimante, un scanner, un disque dur, un vidéoprojecteur. Il vous interpelle pour les assembler et les rendre utilisables.

1. Définir les mots suivants :

Partitionnement :…….

…… **/1 pt**

Périhérique:……

……**.../1pt**

Pilote ou driver : ……

…… **/1pt**

2. Décrire la procédure de mise en marche d'un périphérique……

…….

…….

…….....**/1*3 = 3pts**

3. En se basant sur leur mode de prise en charge par le système d'exploitation, établir une différence entre ces périphériques…….

…….

……

……**./2pts**

4. Nommer et expliquer deux actions qu'on peut effectuer sur un disque dur neuf afin de le rendre utilisable……

……..

……..

……..**/1*2 = 2pts**

PARTIE B : PRATIQUE DE LA SECURITE INFORMATIQUE /10 POINTS

M. BEJELE est le responsable de la sécurité informatique dans une entreprise de la place. Il a mis en place les mesures suivantes afin de renforcer la sécurité au sein de l'entreprise : la protection des fichiers sensibles en écriture (Mesure 1), les sauvegardes journalières de nouvelles données sensibles de

l'entreprise sur le Cloud (Mesure 2), le conditionnement de l'accès à la salle des serveurs par la lecture des empreintes digitales (Mesure 3). Lors de votre stage de vacances dans cette entreprise, il vous présente brièvement son système de sécurité et vous demande de répondre aux consignes suivantes :

1. Définir :

Sécurité informatique……

……

……../**1pt**.

Menace……

……../**1pt**

Vulnérabilité……

……..…/**1pt**

Contre-mesure …….

……../**1pt**

2. Nommer puis expliquer chacun des trois principes fondamentaux de sécurité informatique mis en oeuvre à travers les mesures de M. BEJELE……

……..

……..

……..

……..

……..

…… **/1*3=3pts**

3. Présenter deux avantages de la sécurité informatique……..

……..

……..

……..

……. **/1.5*2=3pts**

Correction de l'épreuve théorique d'informatique

Collège Catholique Bilingue Père Monti

Année scolaire 2024–2025

PARTIE A : UTILISATION DES PÉRIPHÉRIQUES /10 POINTS

1. Définir les mots suivants :

Partitionnement : C'est l'action de diviser un disque dur physique en une ou plusieurs unités logiques indépendantes appelées « partitions » (ex : C :, D :), afin de pouvoir y installer des systèmes d'exploitation ou organiser les données.

Périphérique : C'est tout matériel informatique connecté à l'unité centrale d'un ordinateur, permettant soit d'envoyer des données (entrée), de recevoir des données (sortie), ou de stocker des informations.

Pilote ou driver : C'est un logiciel (programme) qui permet au système d'exploitation de communiquer et d'interagir avec un matériel (périphérique) spécifique connecté à l'ordinateur.

2. Décrire la procédure de mise en marche d'un périphérique.

La procédure de mise en marche d'un périphérique (ex : une imprimante) se fait généralement comme suit :

1. **Connexion physique :** Brancher le périphérique à l'unité centrale (via USB, HDMI, etc.) et à une source d'alimentation électrique si nécessaire.
2. **Mise sous tension :** Appuyer sur le bouton « Power » (marche/arrêt) du périphérique.
3. **Reconnaissance par l'OS :** Le système d'exploitation détecte automatiquement le nouveau matériel (Plug and Play).
4. **Installation du pilote :** Si le pilote n'est pas intégré, le système demande d'insérer un CD d'installation ou de télécharger le pilote approprié.
5. **Test de fonctionnement :** Vérifier que le périphérique est prêt à l'emploi (voyant vert, test d'impression, etc.).

3. En se basant sur leur mode de prise en charge par le système d'exploitation, établir une différence entre ces périphériques.

On peut distinguer les périphériques selon leur mode de prise en charge :

— **Les périphériques Plug and Play (PnP) :** Ils sont reconnus et configurés automatiquement par le système d'exploitation dès leur branchement, sans nécessiter d'installation manuelle de pilotes (ex : souris, clavier, clé USB).
— **Les périphériques non Plug and Play :** Ils nécessitent l'installation manuelle d'un pilote (driver) spécifique fourni par le constructeur pour pouvoir fonctionner correctement (ex : certaines anciennes imprimantes, scanners spécifiques).

4. Nommer et expliquer deux actions qu'on peut effectuer sur un disque dur neuf afin de le rendre utilisable.

Pour rendre un disque dur neuf utilisable, il faut effectuer les deux actions suivantes :

1. **Le partitionnement :** Il consiste à diviser l'espace de stockage brut du disque en une ou plusieurs partitions logiques (ex : une partition pour le système, une autre pour les données). Sans cela, le disque n'est qu'un espace vide non structuré.
2. **Le formatage :** Après le partitionnement, il faut formater chaque partition. Cela consiste à créer un système de fichiers (comme NTFS, FAT32, ou ext4) sur la partition afin que le système d'exploitation puisse y lire, écrire et organiser les fichiers.

PARTIE B : PRATIQUE DE LA SÉCURITÉ INFORMATIQUE /10 POINTS

1. Définir :

Sécurité informatique : C'est l'ensemble des moyens techniques, organisationnels et juridiques mis en œuvre pour protéger les systèmes d'information (matériels, logiciels, données) contre les menaces et les accès non autorisés.

Menace : C'est tout événement, action ou situation susceptible de causer un dommage, une perte ou une altération aux ressources d'un système d'information.

Vulnérabilité : C'est une faiblesse, une faille ou une imperfection dans un système informatique qui peut être exploitée par une menace pour porter atteinte à la sécurité.

Contre-mesure : C'est une mesure de protection, un dispositif ou une procédure mise en place pour prévenir, détecter ou corriger une menace exploitant une vulnérabilité.

2. Nommer puis expliquer chacun des trois principes fondamentaux de sécurité informatique mis en œuvre à travers les mesures de M. BEJELE.

Les trois principes fondamentaux de la sécurité informatique (souvent appelés la triade CIA) sont mis en œuvre par les mesures de M. BEJELE :

1. **La Confidentialité :** Elle vise à garantir que seules les personnes autorisées ont accès aux informations. *Explication :* La protection des fichiers sensibles en écriture (Mesure 1) empêche les utilisateurs non autorisés de consulter ou de modifier ces fichiers.

2. **L'Intégrité :** Elle garantit que les données ne peuvent pas être modifiées ou altérées de manière non autorisée ou accidentelle. *Explication :* La protection en écriture (Mesure 1) assure que les fichiers sensibles restent intacts et ne sont pas corrompus.
3. **La Disponibilité :** Elle assure que les données et les services sont accessibles aux utilisateurs autorisés quand ils en ont besoin. *Explication :* Les sauvegardes journalières de nouvelles données sensibles permettent de restaurer les informations rapidement en cas de panne ou de sinistre, garantissant ainsi leur disponibilité continue.

3. Présenter deux avantages de la sécurité informatique.

La mise en place de la sécurité informatique présente de nombreux avantages, dont :

1. **La protection des données sensibles et de la vie privée :** Elle permet d'éviter le vol, la fuite ou la divulgation d'informations confidentielles (données clients, secrets industriels), préservant ainsi la réputation de l'entreprise et la vie privée des individus.
2. **La continuité et la pérennité des activités :** En prévenant les attaques et en permettant une reprise rapide après un incident (grâce aux sauvegardes), la sécurité informatique évite les interruptions de service coûteuses et assure la survie de l'entreprise.