Exercice 1 :

Définir

1. Système d’information
2. La confidentialité
3. L’intégrité
4. Un compte d’utilisateur
5. Un mot de passe
6. Sécuriser son espace de travail
7. Codage de source
8. Un virus
9. Un antivirus
10. Le chiffrement
11. La cryptographie

Exercice 2 :

1. Quelles sont les menaces auxquelles peut faire face un système d’information ?
2. Comment procéder pour obtenir toutes ces menaces ?
3. Quelles sont les techniques de la sécurisation des systèmes d’information ?
4. Citer les principes fondamentaux de la sécurité informatique ( CID) en définissant chaque terme.
5. Donner quelques avantages de la sécurité informatique.

Exercice 3 :

Dans votre lycée, se trouve un ordinateur qui sert à saisir les épreuves d’examen et aide les élèves à imprimer des exposés. Alors le proviseur redoutant que certains d’entre eux puissent accéder aux épreuves, décide de limiter l’accès à cet appareil aux élèves. Pour cela, il fait appel à vous.

1. Que faire pour éviter que les élèves aient accès aux épreuves séquentielles ?
2. Combien de comptes pourriez vous créer ?
3. Quelle sera la particularité de ces différents comptes d’utilisateurs ?

Exercice 4 :

1. Donner la procédure pour protéger un fichier par mot de passe dans le système windows
2. Donner la procédure pour protéger un dossier par mot de passe dans le système windows

Exercice 5 :

1. Définir compte utilisateur
2. Comment peut-on sécuriser son espace de travail distant ?
3. Combien de compte utilisateur existe- t-il ? Lister les
4. En quoi le compte Administrateur est-il distinct des autres compte utilisateur ?
5. En cryptographie,on distingue deux types de clés, lesquelles ?

**Correction des exercices :**

Exercice 1 :

1. Le système d’information est un ensemble organisé de ressources qui permet de traiter et de collecter les informations grâce à un ordinateur
2. La confidentialité est le fait de s’assurer qu’une information est accessible uniquement par les entités qui ont le droit d’accès
3. C’est le fait de garantir que les données sont bien celles que l’on croît être, consiste à déterminer si les données n’ont pas été altérées durant la communication
4. C’est l’ensemble des ressources informatiques attribuées à un utilisateur ou à un appareil
5. C’est une chaîne de caractères qui sert de code d’accès à un compte utilisateur
6. C’est protéger son espace de travail d’un utilisateur non autorisé
7. C’est l’opération informatique consistant à transformer une suite de bits A en une suite de bits B plus courte pouvant résulter les mêmes informations par un algorithme de décompression.
8. Programme malveillant pouvant nuire au fonctionnement logiciel ou matériel de l’ordinateur
9. Programme conçu pour contenir l’action des virus
10. Opération qui consiste à transformer une donnée qui peut être lue par n’importe qui en une donnée qui ne peut être lue que par son créateur ou destinataire
11. La cryptographie est une discipline alors que le chiffrement est un procédé ( une opération).

Exercice 2 :

1. Les menaces peuvent être : la destruction des données, la corruption ou la falsification des données, le vol ou espionnage des données, l’usage illicite d’un système
2. Mettre sur pied une politique de sécurité informatique, effectuer une analyse de risques, établir une politique de sécurité
3. L’évaluation des vulnérabilités et des tests de pénétration ( pen-test), la sécurisation des données , la surveillance des informations de sécurité
4. C : confidentialité, I : intégrité, D :disponibilité. La disponibilité est le fait de s’assurer que l’information est toujours disponible peu importe le moment choisi.
5. Un système de sécurité doit avant tout :

* Assurer la protection externe et interne du système d’information
* Garantir en tout temps la confidentialité des communications
* S’aligner à la culture de l’entreprise
* Contrôler l’accès à la ressource informatique avec certitude

Exercice 3 :

1. Il faut protéger son espace de travail, sécuriser les données et créer les comptes utilisateurs
2. On pourra créer deux comptes : l’un appartenant au personnel enseignant et l’autre appartenant aux élèves
3. Le compte personnel enseignant est protégé par un mot de passe, le compte des élèves n’est pas protégé par un mot de passe

Exercice 4 :

1. Lorsque le document est saisi, cliquez sur le bouton fichier- enregistrez sous ; sélectionnez un emplacement dans lequel enregistrer le fichier. Dans la boîte de dialogue « enregistrer sous », cliquez sur Outils- Options général. Dans la boîte de dialogue options d’enregistrement, sous partage de fichier, ajoutez des mots de passe pour votre fichier :

* Mot de passe de protection : ce mot de passe est nécessaire pour ouvrir le fichier,
* Mot de passe de réservation d’écriture : tout le monde peut lire le fichier, seules les personnes disposant de ce mot de passe seront aptes à le modifier

1. Windows offre désormais nativement la possibilité de sécuriser un dossier ou un fichier. Pour sécuriser le dossier, faire un clic droit sur ce dossier et choisir «  propriétés ». Dans l’onglet général, choisir « avancé ». Une boîte de dialogue «  attributs avancés » s’ouvre alors. Cochez la case « chiffrer le contenu pour sécuriser les données » et valider. Les autres utilisateurs du système n’auront plus accès aux données de ce dossier et aux fichiers qu’il contient.

Exercice 5 :

1. Un compte utilisateur est un ensemble d’informations indiquant au système d’exploitation les fichiers et dossiers auxquels l’utilisateur concerné peut accéder et modifier.
2. Sécuriser son espace de travail distant revient à :

* Déposer ses fichiers dans un espace privé ;
* Limiter tout risque d’usurpation d’identité ( mot de passe complexe, déconnexion de sa session, etc…)

1. Il existe 3 comptes utilisateur à savoir :

* Compte administrateur,
* Compte utilisateur standard,
* Compte invité.

1. Le compte administrateur est distinct des autres comptes en ce sens que l’administrateur dispose de tous les droits sur tous les autres comptes.
2. On distingue 2 types de clés :

* Les clés symétriques : il s’agit de clés utilisées en même temps pour le chiffrement et le déchiffrement. On parle alors de chiffrement symétrique ou de chiffrement à clés secrète.
* Les clés asymétriques : ici, les clés utilisées pour le chiffrement et le déchiffrement sont différentes. On parle alors de chiffrement asymétrique ou de chiffrement à clé publique.