الجمهورية الجزائرية الديمقراطية الشعبية

REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE

MINISTERE DE L'ENSEIGNEMENT SUPERIEUR
ET DE LA RECHERCHE SCIENTIFIQUE

ECOLE SUPERIEURE DE MANAGEMENT
TLEMCEN

وزارة التعليم العالي والبحث العلمي

المدرسة العليا لإدارة الأعمال
تلمسان

CHARTE DE SECURITE INFORMATIQUE

DE L'ECOLE SUPERIEURE DE MANAGEMENT

DE TLEMCEN v2022

Table des matières

Préambule

L'établissement ''Ecole Supérieure de Management de Tlemcen'' met à disposition de son personnel, de ses étudiants et de ses collaborateurs externes (ci-après dénommés conjointement « **Utilisateurs** »), en fonction des besoins de travail spécifiques à chacun, un accès à des ressources et à de multiples services informatiques. Une mauvaise utilisation de ces moyens augmente les risques d'atteinte à la sécurité des systèmes d'information de l'établissement.

Dans le cadre de la mise en place du référentiel national de sécurité de l'information, il a été décidé d'élaborer une charte de sécurité informatique afin de garantir un seuil minimal de sécurité.

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- **L'établissement** : Ecole supérieure de management de Tlemcen.

- **Ressources informatiques** : ressources et moyens informatiques et moyen de communication électronique, recouvrant tout matériel informatique, câblage, périphériques (tels que imprimantes simples ou multifonctions, webcam, etc.), disque dur externe ou interne, carte mémoire, CD-Rom, clé USB, ordinateur de bureau et portable, tablette, photocopieur, scanner, etc. et toute ressource informatique de toute nature (logiciels, applications, bases de données, etc.) et ce, qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi les moyens de communication électronique recouvrant Internet et les télécommunications (tels que téléphone, équipement sans fil, messagerie, site web, page, forum, etc.).

- **Utilisateur** : toute personne ayant accès (restreint ou non) à certaines ressources informatiques. Ceci inclut :
    - les étudiants
    - les enseignants et enseignants-chercheurs
    - les chercheurs
    - les personnels administratifs ou techniques
    - les organisations syndicales
    - les associations ayant un siège social à l'établissement
    - les visiteurs et les invités

Article 1 : Objet

La présente charte a pour objet de définir les conditions et modalités d'utilisation des ressources informatiques de l'établissement. Elle définit également les règles de sécurité que les utilisateurs doivent respecter.

Article 2 : Champ d'application

La présente charte s'applique à tout utilisateur ayant accès, de manière permanente ou temporaire, aux ressources informatiques de l'établissement

Article 3 : Propriété des ressources informatiques

- Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de l'établissement.
- Toutes les données hébergées dans les équipements de l'établissement ou transitant dans ses réseaux sont la propriété exclusive de l'établissement.

Article 4 : Conditions d'accès aux ressources et au réseau informatique

Tout accès aux ressources et réseaux informatiques de l'établissement est soumis à une procédure d'authentification préalable.

Article 5 : Responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par l'établissement.

Article 6 : Protection des moyens d'authentification

Afin de préserver les moyens d'authentification mis à sa disposition, l'utilisateur doit :

- Définir des mots de passe qui respectent les recommandations suivantes :
  a) Le mot de passe doit être composé de caractères alphanumériques (minuscules, majuscules, numéros et caractères spéciaux).
  b) Le mot de passe doit avoir une taille supérieure à huit (08) caractères
- Veiller à la protection et à la préservation de ses informations secrètes d'authentification.
- Ne pas utiliser les mêmes informations secrètes sur plusieurs comptes.
- Ne pas communiquer ses informations secrètes d'authentification aux tiers.
- Changer périodiquement ses informations secrètes d'authentification.

Article 7 : Utilisation des ressources informatiques

- Les ressources informatiques de l'établissement ne peuvent être utilisées qu'à des fins professionnelles.
- L'utilisateur doit préserver les ressources et les moyens informatiques mis à sa disposition.
- L'utilisateur n'est pas autorisé à installer ou à déployer des applications ou des logiciels sur les moyens ou les ressources informatiques mis à sa disposition.
- En cas de défaillance de ces moyens ou ressources, il doit informer immédiatement la structure en charge de la maintenance.

Article 8 : Obligations de l'établissement vers les utilisateurs

Selon la disponibilité, l'établissement doit :

- Mettre à disposition de l'utilisateur les ressources informatiques nécessaires à l'exécution des missions qui lui incombent.
- Garantir le bon fonctionnement et la disponibilité des ressources informatiques.
- Maintenir la qualité du service fourni aux utilisateurs dans la limite des moyens alloués.
- Informer les utilisateurs des procédures et des politiques applicables en matière de ressources informatiques.
- Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs.
- Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée.
- Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

Article 9 : Obligations de l'utilisateur

L'utilisateur doit :

- Respecter les lois et règlements en vigueur.
- Respecter la présente charte ainsi que les différentes procédures et politiques de l'établissement.
- Appliquer scrupuleusement les mesures et les directives de sécurité informatique de l'établissement.
- Ne pas utiliser ou tenter d'utiliser les comptes d'autrui.
- Signaler sans délai tout fonctionnement suspect ou incident de sécurité.

Article 10 : Sécurité et protection du poste de travail

L'utilisateur doit respecter les consignes de sécurité suivantes :

- Verrouiller l'accès au poste de travail en cas d'absence, même temporaire.
- Alerter les services techniques en cas de découverte d'un nouvel équipement connecté au poste de travail.
- S'assurer que son poste de travail dispose d'un antivirus, et informer le service concerné de toute alerte de sécurité.
- Ne jamais connecter des équipements personnels au poste de travail.
- Scanner tous les supports amovibles connectés au poste de travail avant de les utiliser.
- Eteindre l'ordinateur pendant les périodes d'inactivité prolongée (nuit, weekend, vacances..).
- Ne pas intervenir physiquement sur le matériel (ouvrir les unités centrales, ..).

Article 11 : Utilisation de la messagerie électronique professionnelle

L'établissement met à la disposition des utilisateurs, des comptes de messagerie électronique, qui leurs permettent d'émettre et de recevoir des messages électroniques à caractère professionnel.

La messagerie professionnelle ne peut être utilisée qu'à des fins professionnelles. A cet effet, il est strictement interdit de :

- L'utiliser à des fins personnelles ou partisanes.
- L'utiliser pour l'enregistrement sur les réseaux sociaux, les forums et les sites web.
- Ouvrir les pièces jointes et/ou les liens hypertexte transmis à partir d'adresses mail inconnues.
- Ouvrir la boite mail professionnelle à partir des espaces communautaires d'accès à internet notamment les cybers café.

Lorsque les missions de l'utilisateur nécessitent son enregistrement sur les réseaux sociaux, les forums ou les sites web, une adresse mail dédiée à cet effet lui est attribuée après avis favorable de l'autorité habilitée.

L'utilisateur doit faire preuve de vigilance lors de l'utilisation des courriers électroniques et ceci en s'assurant que :

- L'adresse du destinataire est bien formulée.
- Le destinataire est habilité à accéder au contenu transmis.
- Les bonnes pièces jointes ont été rattachée au document.

Il est strictement interdit d'utiliser les adresses mail personnelles pour la transmission des documents professionnels.

Article 12 : Utilisation d'Internet

Les utilisateurs ayant accès à internet s'engage à :

- Ne pas utiliser intentionnellement ce service à des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires, pornographiques ou illégales.
- Ne pas fournir des informations liées à leur fonction, grade ou responsabilité sur les réseaux sociaux.
- Ne pas surcharger le réseau de l'établissement.
- Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.

Article 13 : Utilisation des appareils mobiles et de supports de stockage

L'utilisateur doit :

- Signaler, à la hiérarchie dans l'immédiat, toute perte ou vol d'un appareil mobile ou support de stockage professionnel.
- Verrouiller toujours les appareils mobiles lorsqu'ils ne sont pas utilisés.
- Désactiver les fonctions Wi-Fi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires.
- Interdiction formelle pour toute personne étrangère à l'établissement de transférer des documents par support amovible, tout échange de document doit se faire par courriel.
- Dans le cas où le volume de données exige le recours à un support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation.
- Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage.
- Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et supports de stockage amovible sur soi.

Article 14 : Mesures de sécurité à appliquer lors des déplacements à l'étranger

- Il est interdit d'utiliser des terminaux (ordinateurs, tablettes) publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier.
- Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage.
- Le missionnaire doit désactiver les fonctions de communication sans fil tel que le Wi-Fi et le Bluetooth des appareils lorsque celle-ci ne sont pas nécessaires.
- Le missionnaire doit supprimer toutes les données professionnelles sensibles, non nécessaire à la mission, de tous les supports amovibles avant tout déplacement à l'étranger.

- Le missionnaire doit informer la hiérarchie et la représentation diplomatique Algérienne en cas d'inspection ou de saisie des équipements informatiques par des autorités étrangères lors des missions à l'étranger.
- Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger à des fins professionnelles.
- Le missionnaire doit mentionner dans les comptes rendus de la mission, la liste des objets connectés offerts lors du déplacement.
- Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de document doit se faire exclusivement par courriel.
- Le missionnaire doit changer les mots de passe utilisés pendant la mission.

Article 15 : Fin de la relation liant l'utilisateur à l'établissement

- Lorsque la relation liant l'utilisateur à l'établissement prend fin, l'utilisateur doit restituer à l'établissement toutes les ressources informatiques matérielles mises à sa disposition.
- L'établissement procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition.

Article 16 : Gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'établissement peut :

- Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation.
- Isoler ou neutraliser provisoirement, toute donnée ou fichier en contradiction avec la charte, ou qui mettrait en péril la sécurité des systèmes d'information.
- Prévenir le responsable hiérarchique.

Article 17 : Non-respect de la charte

Le non-respect des règles définies dans la présente charte, est susceptible d'engager la responsabilité de l'utilisateur, et d'entrainer à son encontre, des mesures disciplinaires proportionnelles à la gravité des faits constatés.

Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatique peuvent :

- Avertir un utilisateur.
- Limiter ou retirer provisoirement les accès d'un utilisateur.
- Effacer, comprimer ou isoler toute donnée ou fichier en contradiction avec la charte, ou qui mettrait en péril la sécurité des systèmes d'information.

Sans préjudice des sanctions disciplinaire, le contrevenant aux dispositions de la présente charte peut faire l'objet de poursuites judiciaires.

Article 18 : Entrée en vigueur

La présente charte entre en vigueur dès sa signature par l'utilisateur. Tout refus de signature interdira l'accès de l'utilisateur aux ressources informatiques de l'établissement.

Fait à Tlemcen le,....07 JUIL. 2022...

Le Directeur

مدير المدرسة
د. سعيدي طارق