MINISTERE DE L'ENSEIGNEMENT SUPERIEUR ET DE LA RECHERCHE SCIENTIFIQUE

UNIVERSITE Abbès Laghrour Khenchela

جامعة عباس لغرور خنشلة

CHARTE INFORMATIQUE

Préambule

L'université Abbès Laghrour Khenchela met à la disposition de ses collaborateurs et usagers des outils informatiques et des moyens de communication afin de leur permettre d'accomplir les missions qui leurs sont assignées.

Une mauvaise utilisation de ces moyens augmente les risques d'atteinte à la sécurité des systèmes d'information de l'UK.

Prenant en compte les préconisations du Ministère de la Poste, des Télécommunications, des Technologies et du Numérique (MPTTN) et de Référentiel National de Sécurité de l'Information (RNSI), ce texte s'inscrit dans le cadre législatif et réglementaire en vigueur relatif à la protection des données à caractère personnel, à l'utilisation des logiciels, aux droits et obligations des utilisateurs des services numériques.

Définition :

UK: Université Abbès Laghrour Khenchela

Utilisateur: toute personne autorisée à accéder et à utiliser les outils informatiques et moyens de communication de l'Université (personnel titulaires ou contractuels, étudiants, intervenants extérieurs, visiteurs, invités, etc.).

Les risques : Désigne les risques qui imposent le respect de certaines règles de sécurité et de bonne conduite. L'imprudence, la négligence ou la malveillance d'un utilisateur peuvent en effet avoir des conséquences graves de nature à engager sa responsabilité civile et/ou pénale ainsi que celle de l'établissement.

- Données à caractère personnel: correspond à toute information relative à une personne physique identifiée ou qui peut être identifiée, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.
- Ressources informatiques: Sont notamment constitutifs de moyens informatiques, les serveurs, stations de travail, réseaux internes et externes de l'UK, les équipements de transmission, les infrastructures de liaison de réseau, Réseau ARN (Réseau Académique de Recherche), les micro-ordinateurs des services, laboratoires, unité de recherche, ainsi que l'ensemble du parc logiciels, des bases de données, des comptes institutionnels, dispositif de contrôle, applications mobiles, des produits multimédias ou des périphériques affectés aux fonctionnement des éléments décrits.
- CSSI : Cellule de sécurité des systèmes d'information.
- CSRICTED: désigne le Centre des Systèmes d'Information et Réseaux, et de Communication et de télé-enseignement et d'enseignement à distance.

Article 1: Objet

La présente charte définit les règles de sécurité et conditions générales d'utilisation des ressources informatiques, et des moyens de communication de l'université UK.

Elle a pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Elle décrit également les sanctions encourues en cas de non respect de ces règles de sécurité, et rappelle les principaux textes de référence.

La charte est diffusée à l'ensemble des utilisateurs par tout moyen et à chaque sortie d'une nouvelle version. A ce titre, elle est publiée sur le site web officiel de l'Université. Elle est systématiquement communiquée à tout nouvel arrivant.

Article 2: Champ d'application

La présente charte s'applique à toute personne ayant accès, de manière permanente ou temporaire, aux ressources informatiques de l'UK.

Article 3: De la propriété des ressources informatiques

- Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive de l'UK;

- Toutes les données hébergées dans les équipements de l'UK ou transitant dans ses réseaux sont la propriété exclusive de l'université UK.

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

- Tout accès aux ressources et réseaux informatiques de l'UK est soumis à une procédure de signature de la présente charte.
- Aucune disposition des chartes informatiques ou des règles régissant des systèmes informatiques en vigueur au sein des différents services et composants de l'université UK ne peut faire obstacle à l'application de la présente charte.

Article 5: Responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation locale ou distante des ressources informatiques mis à sa disposition par l'UK, ainsi que de l'ensemble des informations qu'il met à la disposition du public via les ressources informatiques de l'UK.

- Chaque utilisateur reconnaît que tout dommage créé de sa part à l'Université UK ou à des tiers à la suite d'une violation de la présente Charte engagera sa responsabilité.

Article 6: Protection des moyens d'authentification

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

- Veiller à la protection et à la préservation de ses informations secrètes d'authentification
- Changer périodiquement ses informations secrètes d'authentification;
- Veiller à la confidentialité des comptes utilisateurs, codes ou mots de passe ou tout autre dispositif de contrôle d'accès qui leur sont confiés à titre personnel;
- Se déconnecter obligatoirement dès la fin de chaque période de travail ;

Ne pas installer de logiciel sans l'accord formel du responsable du système ;

Ne pas connecter du matériel réseau sans l'accord formel du responsable réseau ;

- S'assurer de l'activation et la mise à jour périodique de l'antivirus sur son poste de travail ;

Ne pas procéder à aucune opération susceptible d'altérer ou d'interrompre le fonctionnement normal du système informatique de l'université;

Et d'une manière générale, Il est strictement interdit de communiquer ses informations secrètes d'authentification aux tiers.

Article 7: Utilisation des ressources informatiques

- Les ressources informatiques de l'UK ne peuvent être utilisées qu'à des fins professionnelles ;
- L'utilisateur doit préserver les ressources et les moyens 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'UK vers les utilisateurs

L'université UK doit :

- Mettre à disposition de l'utilisateur les ressources informatiques nécessaire 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;
- Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

Article 9: Obligations de l'utilisateur

Puisque La sécurité est l'affaire de tous, l'utilisateur doit :

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

Article 10: De la sécurité et de la protection des ressources informatiques

L'utilisateur doit respecter scrupuleusement les consignes de sécurité suivantes :

L'accès physique aux salles informatiques contenants les équipements de connexion réseau administrables est strictement interdit sans autorisation.

- 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, ...).

- Demander un onduleur pour protéger le poste de travail de l'altération des données en cas d'un incident électrique.

Utiliser autant que possible les logiciels Open source dans les salles de travaux pratiques

Article 11: De l'utilisation de la messagerie électronique professionnelle

L'UK met à la disposition des utilisateurs des comptes de messageries électroniques 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;
- Utiliser les adresses mail personnelles pour la transmission des documents professionnels;

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.
- Fermer la session après chaque consultation du courrier électronique.

Article 12: De l'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'UK;
- Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.
- Vérifier la validité des certificats de confiance pour tout site web consulté.

Article 13: 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'UK 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;

Il 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 ;

Il 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'UK ou changement de mission

- Lorsque la relation liant l'utilisateur à l'UK prend fin, l'utilisateur doit restituer à L'UK toutes les ressources informatiques matérielles mises à sa disposition;
- L'UK procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition par l'UK.
- En cas de changement de mission, l'utilisateur doit restituer au responsable hiérarchique toutes les ressources informatiques mises à sa disposition, à cet effet le responsable doit signaler le changement au service concerné.

Article 16: Gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'UK 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: Du 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 informatiques peuvent :

Avertir un utilisateur;

- Limiter ou retirer provisoirement les accès d'un utilisateur;
- Effacer, comprimer ou isoler toute données ou fichier en contradiction avec la présente 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: Modification de la charte

Le signataire est informé que cette charte peut être modifiée à tout moment. Les modifications apportées lui seront notifiées périodiquement.

Article 19: Entrée en vigueur

Cette Charte entre vigueur dès sa signature par l'utilisateur. Tout refus de signature interdira l'accès de l'utilisateur aux ressources informatiques de l'université UK.