الجمهورية الجزائرية الديمقراطية الشعبية

People's Democratic Republic of Algeria

Ministry of Higher Education& Scientific Research

University Center of Aflou El-Cherif Bouchoucha

وزارة التعليم العالي والبحث العلمي

المركز الجامعي الشريف بوشوشة آفلو

Charte de sécurité informatique

Préambule

Le centre universitaire d'Aflou met à la disposition des utilisateurs des moyens informatiques 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 du C-U -AFLOU.

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.

Concepts terminologiques :

- ***Utilisateur**: Conformément aux dispositions de cette charte, un utilisateur est toute personne autorisée à accéder et à utiliser les outils informatiques et moyens de communication du C-U-AFLOU (personnel titulaires ou contractuels, étudiants, intervenants extérieurs, visiteurs, invités, etc.).*
- ***CSSI** : Cellule de sécurité des systèmes d'information.*
- ***CSRICTED** : désigne le Centre des systèmes d'information, et réseaux, et de communications, et de télécommunication et de l'enseignement à distance.*
- ***BSN** : Bureau de stratégie de numérique, qu'est une entité consultative chargée d'accompagner la mise en œuvre pratique du processus de numérisation au niveau du centre universitaire, conformément aux dispositions et règles de cette charte.*
- ***CATI** : Centre d'appui à la technologique et a l'innovation, est une entité principale chargée de l'inscription des brevets et de la protection des idées novatrices des étudiants et des chercheurs.*
- ***INAPI** : Institut national algérien de la propriété industrielle.*
- ***ONDA** : Office national des droits d'auteur.*
- ***ARN** : Réseau de recherche académique (Academic Research Network).*

- ***Ressources informatiques*** *: Sont notamment constitutifs de moyens informatiques, les serveurs, stations de travail, réseaux internes et externes du C-U-AFLOU, 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.*
- ***Risques*** *: Ils font référence aux risques qui nécessitent le respect de règles de sécurité et de bon comportement. L'imprudence, la négligence ou la malveillance de l'utilisateur peuvent entraîner de graves conséquences, telles que l'engagement de sa responsabilité civile et/ou pénale, ainsi que celle de l'institution.*
- ***Données à caractère personnel*** *: Elles désignent toute information se rapportant à une personne physique identifiée ou qui peut être identifiable, notamment par référence à un identifiant ou à un ou plusieurs éléments spécifiques, conformément aux dispositions de la loi 18-07 du 10/06/2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.*

Article 1 : Principes fondamentaux

Le Centre Universitaire EL Chérif Bouechoucha met à la disposition de son personnel et de ses utilisateurs des outils, des technologies de l'information et des moyens de communication pour leur permettre d'accomplir leurs missions. Ce texte s'inscrit dans le cadre législatif et réglementaire en vigueur concernant la protection des données, l'utilisation des logiciels et les droits et obligations des utilisateurs de services numériques, notamment ceux énoncés par l'arrêté 03-05 du 19/07/2003 relatif aux droits d'auteur et aux droits voisins.

Article 2 : Objectifs.

Cette charte établit les règles de sécurité, les conditions générales et les dispositions d'utilisation des ressources informatiques et des moyens de communication au sein du centre universitaire. Elle vise à sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes de sécurité et de confidentialité des informations traitées. Elle décrit également les sanctions encourues en cas de non-respect de ces règles de sécurité et mentionne les références législatives principales. La charte est distribuée à tous les utilisateurs par tout moyen et chaque fois qu'une nouvelle version est publiée. Elle est également publiée sur le site officiel du centre et est automatiquement transmise à tous les nouveaux arrivants au centre.

Article 3: Champ d'application

La présente charte s'applique à toute personne ayant accès, de manière permanente ou temporaire, aux ressources informatiques du ***Centre Universitaire ElCherif Bouchoucha -Aflou-***

Article 4: de la propriété des ressources informatiques

- *Toutes les ressources informatiques mises à la disposition des utilisateurs sont la propriété exclusive du* ***Centre Universitaire ElCherif Bouchoucha Aflou*** *;*
- *Toutes les données hébergées dans les équipements du* ***Centre Universitaire*** *ou transitant dans ses réseaux sont la propriété exclusive du* ***Centre***

Article 5 : Conditions d'accès aux ressources et au réseau informatique

Tout accès aux ressources et réseaux informatiques du ***Centre Universitaire ElCherif Bouchoucha -Aflou-*** *est soumis à une procédure d'authentification préalable.*

Article 6 : responsabilité de l'utilisateur

L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par le ***Centre Universitaire ElCherif Bouchoucha -Aflou-****.*

Article 7 : 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*
- *Il est strictement interdit de communiquer ses informations secrètes d'authentification aux tiers*
- *Déconnexion à la fin de chaque session de travail.*
- *Ne pas effectuer de modifications sur les données sans obtenir préalablement l'autorisation de l'administrateur CSSI.*
- *Ne pas installer de logiciels sans l'autorisation de l'administrateur CSSI.*
- *Ne pas connecter d'équipements réseau sans l'autorisation de l'administrateur CSSI.*
- *S'assurer d'activer et de mettre à jour régulièrement le logiciel antivirus sur sa station de travail.*
- *Ne pas effectuer d'actions susceptibles de modifier ou d'interrompre le fonctionnement normal du système d'information du centre.*
- *Il est strictement interdit de divulguer ses informations d'identification confidentielles à des tiers.*

Article 8 : Utilisation des ressources informatiques

- *Les ressources informatiques de l'organisme 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 ;*
- *Chaque utilisateur est seul responsable de son compte, et doit assumer les conséquences de ce qui est publié par ce compte dans les limites de sa responsabilité.*
- *En cas de défaillance de ces moyens ou ressources, il doit informer immédiatement la structure en charge de la maintenance.*

Article 9 : Obligations du C-U-AFLOU vers les utilisateurs

Le centre doit :

- *La mise en place d'un espace virtuel d'apprentissage sur le site officiel du centre universitaire, qui est couvert par les mesures de protection et de sécurité informatique nécessaires.*
- *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 ;*
- *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 10 : 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 du CUA;*
- *Appliquer scrupuleusement les mesures et les directives de sécurité informatique du CUA;*
- *Ne pas utiliser ou tenter d'utiliser les comptes d'autrui ;*
- *Signaler sans délai tout fonctionnement suspect ou incident de sécurité.*

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

Le centre universitaire 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 ;*
- *Il est strictement interdit d'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.*

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'organisme ;*
- *Faire preuve de prudence lors du téléchargement des fichiers, et s'assurer de les scanner par un antivirus.*

Article 13 : de la sécurité et de la protection du poste de travail

L'utilisateur doit respecter scrupuleusement 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 14 : 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'organisme 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 15 : 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 16: Protection des œuvres numériques appartenant au Centre Universitaire

Dans le cadre du respect des règles et du dispositions de l'Ordonnance N° : 03-05 du 19/07/2003 relative aux droits d'auteur et aux droits voisins, ainsi que les dispositions de l'Arrêté Ministériel N° 1082 du Ministère de l'Enseignement Supérieur, définissant les règles relatives à la prévention du vol scientifique, les œuvres numériques détenues par le Centre Universitaire sont soumises à une protection légale et à une surveillance nécessaire, sous le nom de la base de données des travaux réalisés par les étudiants et les professeurs.

Les œuvres numériques suivantes sont notamment incluses dans ce cadre :

- *Toutes les publications scientifiques ou pédagogiques produites par les professeurs universitaires affiliés au Centre Universitaire et publiées sur le site officiel du Centre Universitaire.*
- *Les mémoires de licence, de master et de doctorat produits par les étudiants du Centre Universitaire.*
- *Les projets de fin d'études pour les certificats "Startup" et "Brevet d'invention", en coordination avec les institutions INAPI et ONDA, afin d'accélérer l'enregistrement légal et la protection nécessaire de ces projets, ainsi que le suivi des droits de propriété intellectuelle et industrielle des étudiants et des chercheurs, et de surmonter toutes les difficultés qui peuvent survenir tout au long de ces étapes.*
- *Les travaux publiés lors de conférences internationales et nationales organisées au Centre Universitaire.*
- *Les cours et divers travaux pédagogiques publiés par les professeurs sur la plateforme d'apprentissage virtuelle du Centre Universitaire.*
- *Les rapports de stages sur le terrain réalisés par les professeurs et les étudiants à l'étranger.*
- *Les projets de recherche.*

Article 17: Mécanismes de protection des œuvres numériques appartenant au Centre Universitaire

Conformément aux dispositions de l'Article 06 de l'Arrêté Ministériel n° 1082, qui oblige toutes les institutions d'enseignement supérieur et les institutions de recherche à mettre en place des mesures de contrôle, les éléments suivants doivent être assurés :

- *Garantir la surveillance de la base de données des travaux réalisés par les étudiants et les professeurs.*
- *Mettre régulièrement à jour la base de données numérique des noms des professeurs affiliés au Centre Universitaire selon leurs départements et spécialités, y compris leurs CV et leurs intérêts scientifiques et de recherche, afin de bénéficier de leur expertise dans l'évaluation des travaux de recherche scientifique et des activités.*
- *Activer des logiciels d'information permettant de détecter le vol scientifique en arabe et dans d'autres langues étrangères, y compris des logiciels disponibles gratuitement sur Internet et d'autres logiciels disponibles, en privilégiant les logiciels algériens ou locaux lorsque cela est nécessaire.*

Article 18 : fin de la relation liant l'utilisateur au Centre universitaire

- *Lorsque la relation liant l'utilisateur au C-U-A prend fin, l'utilisateur doit restituer au centre toutes les ressources informatiques matérielles mises à sa disposition ;*
- *procédera à la suppression de l'ensemble des accès logiques de l'utilisateur aux ressources informatiques mises à sa disposition par le centre.*

Article 19 : gestion des incidents

En cas d'incident pouvant affecter la sécurité, l'organisme 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 20 : 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 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 21 : entrée en vigueur

Cette Charte entre en vigueur dès sa signature par le directeur du Centre Universitaire et par l'utilisateur. En cas de refus de l'utilisateur de signer le pacte, il est interdit à l'utilisateur d'accéder aux ressources informatiques de l'établissement.

Les dispositions de ce pacte sont soumises à modification chaque fois que cela est nécessaire, et toutes les parties concernées sont informées de ces modifications via le site officiel du Centre Universitaire.

Les demandes de modification peuvent être faites par:

- *Le directeur du Centre Universitaire*
- *Le responsable du CSSI (Centre de Services et de Systèmes d'Information)*

Le directeur