Charte informatique

de

L'Université de Ferhat Abbas Sétif 1

Version 1.0

Edition 2024

Cette charte informatique est modifiable et ajustable suivant les développements technologiques et les textes règlementaires en vigueur

L'université Ferhat Abbas Sétif 1 met en œuvre un système d'information et de communication nécessaire au bon déroulement des activités académiques, pédagogiques, scientifiques et professionnelles, comprenant notamment un réseau informatique et téléphonique, logiciels, site et plateformes Web, messagerie ainsi que des équipements informatiques fixes et mobiles.

L'utilisation du système d'information et de communication et des ressources informatiques doit être effectué exclusivement à des fins académiques et professionnelles, sauf par exception autorisé par les services concernés. Par ailleurs, des tierces au UFAS1 peuvent également avoir accès aux équipements informatiques et aux systèmes d'information et de communication du UFAS1.

La charte informatique vise à définir les règles et les droits d'utilisation de l'ensemble des moyens informatiques disponibles au sein des structures de l'université Ferhat Abbas - Sétif1, et à préciser les responsabilités des utilisateurs (enseignants, étudiants et ATS) afin de permettre un usage convenable et optimal des ressources informatiques disponibles, en garantissant un niveau minimal de sécurité adapté au milieu universitaire. De même que cette charte vise également à sensibiliser les utilisateurs aux risques liés à l'intégrité et de confidentialité des informations traitées et des ressources utilisées.

La charte est diffusée à l'ensemble des utilisateurs et ces derniers sont informés systématiquement de chaque mise à jour apportée. À ce titre, elle est systématiquement communiquée à tous les utilisateurs, et disponible sur le site institutionnel de l'Université. Des actions de communication, d'information et de sensibilisation internes sont organisées régulièrement afin de maintenir un niveau d'information suffisant sur les bonnes pratiques recommandées.

1. Objectif

Cette charte a pour objectifs :

1.1 De sensibiliser les utilisateurs aux risques liés à la sécurité informatique en matière de libertés et de vie privée, notamment à travers les traitements de données à caractère personnel qu'ils sont amenés à effectuer.

1.2 D'informer les utilisateurs surs : Les usages permis des moyens informatiques mis à sa disposition. Les règles de sécurité en vigueur. Les mesures de contrôle prises par l'UFAS1. Les sanctions éventuellement encourues par les utilisateurs.

1.3 De formaliser les règles générales de sécurité que les utilisateurs s'engagent à respecter, en contrepartie de la mise à disposition des systèmes d'information et des équipements informatiques, et ainsi de déterminer les droits et devoirs des utilisateurs.

2. Définition de concepts

2.1 Ressources informatiques

Elles Incluent tous les moyens matériels et logiciels, ainsi que l'accès au web, l'intranet et la messagerie électronique, disponibles au sein de l'université ou accessibles de l'extérieur du campus. On mentionne notamment les réseaux, les serveurs, les stations de travail, les logiciels, les applications, site et plateformes Web, les bases de données, les routeurs, les commutateurs, les points d'accès Wi-Fi, les câbles, imprimantes et scanner, téléphone IP, disque dur et flash disque, etc.

2.2 Propriété des ressources informatiques

Toutes les ressources informatiques fournies aux utilisateurs appartiennent exclusivement à l'université Ferhat Abbas - Sétif 1. De même, toutes les données stockées sur les équipements de l'université ou transitant dans ses réseaux sont la propriété exclusive de l'université.

2.3 Utilisateurs concernés

Les règles et droits d'accès sont applicables à tous les utilisateurs ayant un accès permanent ou temporaire aux ressources de l'université : enseignants, étudiants, doctorants, chercheurs, employés et agents administratifs et techniques, enseignants vacataire, stagiaires, invités, etc.

2.4 Services Internet

La mise à disposition par des serveurs locaux ou de moyens d'échanges et d'informations diverses : web, messagerie, forum, téléphonie IP, visioconférence …etc.

3. Champs d'application

Les règles définies dans cette charte s'appliquent à tous les moyens informatiques proposés par l'université et à tous les utilisateurs de ces moyens dans tous les campus et les toutes les structures de l'UFAS, à l'intérieur et à l'extérieur du campus universitaire.

4. Droit d'accès aux ressources informatique

4.1 L'accès pour chaque utilisateur est accordé dans la limite des prérogatives qui lui sont attribuées. Ce droit est personnel et ne peut être cédé même temporairement à un tiers, il est matérialisé par la création ***d'identifiants nominatifs et confidentiels pour chaque utilisateur des ressources mises à disposition.***

4.2 Le droit d'accès peut être limité ou retiré, par mesure conservatoire, si le comportement de l'utilisateur n'est pas en adéquation avec la présente charte.

4.3 Un utilisateur ne peut en aucun cas permettre à une autre personne, d'accéder aux ressources de l'université au moyen de ses identifiants. Dans cette situation l'utilisateur sera responsable des actions effectuées avec ses identifiants.

4.4 Toute perte, vol ou divulgation d'informations d'authentification, doivent être immédiatement signaler à l'université.

5. Conditions d'utilisation

5.1 Les ressources informatiques mises à disposition par l'université ne peuvent être utilisées qu'à des fins professionnelles.

5.2 L'accès à une ressource informatique n'est permis qu'aux personnes dûment autorisés et identifiées de l'université. Des procédures d'autorisation préalable de la part de la structure responsable de la ressource en question peuvent être exigées pour des applications particulières.

5.3 Le droit d'accès est limité à des activités conformes de ladite structure et ne peut être utilisé dans d'autres activités hors du cadre défini.

6. Responsabilités de l'université

6.1 Mettre à dispositions de l'utilisateur les ressources informatiques nécessaires à l'exécution des missions qui lui incombent.

6.2 Garantir le bon fonctionnement et la disponibilité des ressources informatiques.

6.3 Maintenir la qualité de service fourni aux utilisateurs dans la limite des moyens alloués.

6.4 Informer les utilisateurs des procédures et de politique applicable en matière de ressources informatiques.

6.5 Mettre en œuvre les moyens nécessaires pour assurer la confidentialité et l'intégrité des documents et des échanges électroniques des utilisateurs.

6.6 Informer les utilisateurs que les activités sur le réseau et les systèmes font l'objet d'une surveillance automatisée.

6.7 Sensibiliser les utilisateurs sur les risques liés à la sécurité informatique.

7. Responsabilité de l'utilisateur

7.1 Respecter les lois et les règlements en vigueur.
7.2 Respecter la présente charte ainsi que les différentes procédures et politiques de l'organisme.
7.3 Appliquer scrupuleusement les mesures et les directives de sécurité informatique de l'organisme.
7.4 Ne pas utiliser ou tenter d'utiliser les comptes d'autrui.
7.5 L'utilisateur est seul responsable de toute utilisation des moyens d'authentification mis à sa disposition par l'université.
7.6 En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.
7.7 L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition.
7.8 L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'université.
7.9 L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données.

8. Règles de déontologie informatique

Chaque utilisateur s'engage à respecter les règles de la déontologie informatique et à ne pas effectuer intentionnellement des opérations qui pourraient avoir pour conséquences :

8.1 De masquer sa véritable identité.
8.2 De porter atteinte à l'image, la réputation et l'intégrité de l'université.
8.3 D'altérer, de modifier des données ou d'accéder à des informations appartenant à d'autres utilisateurs du réseau ou à l'université, sans leur consentement.
8.4 D'interrompre ou de perturber le fonctionnement normal du réseau ou d'un des systèmes connectés au réseau.
8.5 De modifier ou de détruire des informations sur un des systèmes.
8.6 De se connecter ou d'essayer de se connecter à un site sans y être autorisé.
8.7 De tenter d'intercepter des communications entre tiers.

9. Protection du poste de travail

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

10. Messagerie électronique

10.1 L'utilisateur s'engage à ne pas partager les accès de son compte de messagerie fournis par l'université avec une autre personne.
10.2 L'utilisateur s'engage à avoir un mot de passe robuste : alphanumériques avec des caractères spéciaux et des majuscules, et à le modifier régulièrement.

10.3 L'adresse de messagerie ne peut être utilisée dans des sites qui peuvent présenter des risques de sécurité pour le compte de l'utilisateur ou les ressources de l'université.

10.4 Chaque utilisateur doit créer sa propre signature comportant ses informations de contact et l'utiliser dans chaque envoi de message.

10.5 Ne pas ouvrir des fichiers ou des liens transmis à partir d'adresses email inconnues.

10.6 Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables.

10.7 L'utilisation et la gestion du compte de messagerie est de la responsabilité de l'utilisateur.

10.8 Ne pas utiliser la messagerie pour des fins personnels ou partisanes.

10.9 Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les utilisateurs sont invités à informer le centre des systèmes et des réseaux des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

10.10 L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer au centre des systèmes et des réseaux.

10.11 Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception ou signés électroniquement.

10.12 Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires fixé par le centre des systèmes et des réseaux. Cette limite est susceptible d'être levée temporairement sur demande.

10.13 De même, la taille, le nombre et le type des pièces jointes peuvent être limités par le centre des systèmes et des réseaux pour éviter l'engorgement du système de messagerie.

11. Internet, Intranet et connectivité

11.1 L'accès au web via l'infrastructure de l'université est ouvert à des usages pédagogiques, de recherche et de gouvernance.

11.2 Ne pas utiliser ce service pour des fins malveillantes, obscènes, frauduleuses, haineuses, diffamatoires ou illégales.

11.3 Tout téléchargement de fichiers, notamment de sons, d'images ou de vidéos, sur le web doit s'effectuer dans le respect des droits de la propriété intellectuelle et ne doit pas sortir du cadre de l'activité académique, pédagogique, de recherche et de gouvernance.

11.4 Le téléchargement de fichiers vidéo, audio ou de logiciels de grandes tailles et qui peuvent générer une lenteur d'accès au web pour les autres utilisateurs est strictement interdit.

11.5 Toute publication de pages d'informations ou de documents sur les sites Internet ou Intranet de l'UFAS doit être validée par un responsable de site ou responsable de publication nommément désigné.

11.6 L'utilisation du réseau ou d'un PC, serveur, modem, routeur ou autre équipement pour l'offre d'un service disponible depuis le web comme RDP (Remote Desktop Protocol) est strictement interdite.

11.7 Ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers.

11.8 L'utilisateur ne doit pas déposer des données sur un serveur interne ou ouvert au grand public (google, free, orange, …) ou sur le poste de travail d'un autre utilisateur sans y être autorisé par les responsables habilités.

11.9 L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

11.10 L'insertion de points d'accès, modem, switch dans le réseau est soumis à l'autorisation préalable de l'ingénieur réseau.

13 Des appareils mobiles et de support de stockages

L'utilisateur doit :

13.1 Signaler, à la hiérarchie dans l'immédiat, toute perte ou vol d'un appareil mobile ou support de stockage professionnel.

13.2 Verrouiller toujours les appareils mobiles lorsqu'ils ne sont pas utilisés.

13.3 Désactiver les fonctions Wifi et Bluetooth des appareils lorsque celles-ci ne sont pas nécessaires.

13.4 Interdiction formelle pour toute personnes étrangères à l'université de transférer des documents par support amovible, tout échange de document doit se faire par courriel. Dans le cas de volume de données exige le recours à support amovible, ce dernier doit être analysé par les services compétents avant toute utilisation.

13.5 Chiffrer les données confidentielles contenues dans des appareils mobiles et des supports de stockage.

13.6 Lors des déplacements professionnels, l'utilisateur doit garder ses appareils mobiles et support de stockage amovibles sur soi.

14. Médias sociaux

14.1 Les comptes officiels doivent être gérés par des personnes désignées par l'université.

14.2 Toute publication doit être conforme aux valeurs et à l'image de l'université.

14.3 L'usage des réseaux sociaux durant le temps de travail doit rester limité à un usage professionnel.

14.4 Ne partagez pas d'informations confidentielles concernant l'université, ses membres ou ses activités sans autorisation.

14.5 Les opinions partagées en ligne doivent être les vôtres et ne pas engager la responsabilité de l'université, sauf autorisation explicite.

14.6 Respectez les droits d'auteur et les propriétés intellectuelles lors du partage de contenus.

14.7 Signalez tout comportement inapproprié aux autorités compétentes de l'université.

15. Mesures de sécurité à appliquer lors des déplacements à l'étranger

15.1 Il est interdit d'utiliser des terminaux publics ou partagés pour accéder au compte de messagerie professionnelle ou aux applications métier.

15.2 Le missionnaire doit désactiver les fonctions de communication sans fil tel que le Wifi et le Bluetooth des appareils lorsque celle-ci ne sont pas nécessaires.

15.3 Le missionnaire doit garder sur lui, en permanence, son terminal professionnel ainsi que les supports de stockage.

15.4 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.

15.5 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.

15.6 Il est interdit d'utiliser des équipements offerts lors d'un déplacement à l'étranger pour des fins personnelles.

15.7 Il doit mentionner dans les comptes rendus de la mission, la liste des objets connectés offerts lors du déplacement.

15.8 Il est formellement interdit qu'un transfert des documents par un étranger se fasse via des supports de stockage amovibles. Tout échange de documents doit se faire exclusivement par courriel.

15.9 Le missionnaire doit changer les mots de passe utilisés pendant la mission.

16. Sécurité

Les utilisateurs doivent veiller au respect strict des lois, réglementations et consignes de sécurité informatique en vigueur. Ils doivent notamment verrouiller leur poste de travail en cas d'absence, surtout en cas d'absence prolonger, s'interdire de connecter des équipements personnels, et disposer d'outils scanner et antivirus pour tous supports amovibles.

Les utilisateurs sont tenus de respecter les consignes suivantes :

16.1 Veiller à ne pas injecter des fichiers volumineux dans les réseaux informatiques.

16.2 Veiller à ne pas injecter des virus dans le réseau provenant de son flash disque, de sites Web malveillants ou de son compte de messagerie.

16.3 Bien vérifier les sites Web auxquels il accède et éviter les sites malveillants.

L'UFAS1 se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.

N.B. Un guide de bonne pratique lié à la sécurité informatique de l'UFAS1 a été établis et doit être respecté par tout utilisateur de ressources informatique.

17. Cadre juridique

Les utilisateurs des ressources informatiques de l'université, s'engagent à respecter les lois sur la propriété littéraire et artistique, ainsi que les lois qui lui sont associées sur la responsabilité civile, pénale et professionnelle. Ceci implique plus particulièrement le respect des obligations suivantes (sans que cela constitue une liste limitative) :

17.1 Le respect du droit d'auteur (droit moral, patrimonial, de diffusion).

17.2 Le respect de la vie privée ou du droit à l'image d'autrui.

17.3 L'interdiction de l'usurpation d'identité, du vol, de la diffamation, de la diffusion d'informations personnelles, confidentielles ou constituant une violation de la personnalité physique ou morale.

17.4 Le respect des exigences de la loi "Informatique et Libertés"(Loi n° 03-17, Ordonnance n° 03-05 du 19 juillet 2003 : Protection des droits d'auteur et droits voisins et Loi n° 18-07 du 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel).

18. Confidentialité

18.1 Les données d'un utilisateur, sauf risque ou événement particulier, doivent être considérées comme privées si elles sont clairement identifiées comme telles. L'accès aux données privées d'un utilisateur exige l'accord de ce dernier.

18.2 Tout utilisateur autorisé à accéder aux données et aux ressources informatiques de l'Université s'engage à maintenir confidentielle l'information à laquelle il accède dans le cadre de ses fonctions.

18.3 L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

18.4 Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisis par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

19. Gestion des incidents

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

19.1 Déconnecter un utilisateur, avec ou sans préavis selon la gravité de la situation.

19.2 Isoler ou neutraliser provisoirement toute donnée ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité des systèmes d'informations.

19.3 Prévenir le responsable hiérarchique.

20. Sanctions applicables

20.1 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.

20.2 Sous réserve que soit informé le responsable hiérarchique, les responsables de la sécurité informatiques peuvent avertir un utilisateur, limiter ou retirer provisoirement ses accès, et effacer ou comprimer ou isoler toute données ou fichier en contradiction avec la charte ou qui mettrait en péril la sécurité de systèmes d'information.

20.3 Les cas de fraude, de non-respect des règles, les atteintes au bon fonctionnement de l'établissement sont soumises à la commission disciplinaire de l'UFAS1 qui prononce les sanctions.

21. Fin de la relation liant l'utilisateur à l'UFAS

21.1 Lorsque la relation liant l'utilisateur à l'université prend fin, l'utilisateur doit restituer à l'organisme toutes les ressources informatiques matérielles mises à sa disposition.

21.2 L'organisme procédera à la suppression de l'ensemble des ressources informatiques mises à sa disposition par l'organisme.

22. Entrée en vigueur de la charte

La présente charte prendra effet dès son adoption par les instances délibérantes de l'université : Conseil Scientifique et Conseil d'Administration.

Elle sera publiée par les moyens légaux de l'université et sera intégrée dans le règlement intérieur de l'UFAS.

23. Engagement individuel

Tous les membres de la famille universitaire, enseignants, étudiants, agents administratifs et technique, doivent affirmer leur acceptation et engagement au respect de toutes les dispositions énoncées dans cette charte.

Ils doivent renseigner les champs d'information du cadre ci-dessous, apposer la mention 'lu et accepté' et signer le document.

Je soussigné,

Nom et prénom : ……

Profession/Grade : ……

Faculté/Service : ……

Département : ……

Utilisateur des ressources informatiques et réseaux de l'Université Ferhat Abbas Sétif 1, certifie et affirme avoir pris connaissance de la présente charte et m'engage à la respecter.

Date et signature :

Textes de références :

Texte légal ou réglementation.	**Références**
Réglementation relative aux mesures cryptographiques.	**Décret exécutif n°16-61 du 02 Joumada El Oula 1437 correspondant au 11 février 2016 modifiant et complétant le décret exécutif n° 09-410 du 23 Dhou El-Hidja 1430 correspondant au 10 décembre 2009 fixant les règles de sécurité applicables aux activités portant sur les équipements sensibles.**
Les règles générales relatives à la poste et aux communications électroniques	**loi n°18-04 du 24 Chaâbane 1439 correspondant au 10 mai 2018 fixant les règles générales relatives à la poste et aux communications électroniques.**
Propriété intellectuelle (Les logiciels)	**Ordonnance n°03-05 du 19 Joumada EL Oula 1424 correspondant au 19 juillet 2003 relative aux droits d'auteur et aux droits voisins.**
Certification électronique	**Loi n°15-04 du 11 Rabie Ethani 1436 correspondant au 1er Février 2015 fixant les règles générales relatives à la signature et à la certification électroniques. Décret n°2016-134 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant l'organisation, le fonctionnement et les missions des services techniques et administratifs de l'Autorité nationale de certification électronique. Décret n°2016-**

	135 du 17 Rajab 1437 correspondant au 25 avril 2016 fixant la nature, la composition, l'organisation et le fonctionnement de l'Autorité gouvernementale de certification électronique.
Protection des données à caractère personnel.	**Loi n° 18-07 du 25 Ramadhan 1439 correspondant au 10 juin 2018 relative à la protection des personnes physiques dans le traitement des données à caractère personnel.**
Les infractions liées aux technologies de l'information et de la communication	**Loi n° 09-04 du 14 Chaâbane 1430 correspondant au 05 aout 2009 portant règles particulières relatives à la prévention et à la lutte contre les infractions liées aux technologies de l'information et de la communication.**
Lutte contre la cybercriminalité.	**Décret présidentiel n° 14-252 du 13 Dhou El Kaada 1435 correspondant au 8 septembre 2014 portant ratification de la convention arabe pour la lutte contre la cybercriminalité.**