CHARTE INFORMATIQUE

Étudiants

Charte de sécurité du système d'information à l'attention des étudiants de l'ÉCOLE NATIONALE SUPÉRIEURE D'ARCHITECTURE de Clermont-Ferrand (ENSACF)

SOMMAIRE

ANNEXES

TITRE 1 : CADRE GÉNÉRAL

ARTICLE 1 : PROPOS LIMINAIRES

La présente Charte Informatique est communément appelée *charte utilisateur*, *charte de bon usage des outils informatiques et de télécommunications* ou encore *charte des usages numériques.* Toutes ces dénominations désignent ce même document.

Cette Charte est à la fois un code de bonne conduite et un texte règlementaire, avec une portée juridique pour les personnes qui y sont soumises. À ce titre, elle est intégrée au Règlement Intérieur de l'École Nationale Supérieure d'Architecture de Clermont-Ferrand (ENSACF) et en a la même force obligatoire.

La présente Charte vise à protéger l'ensemble des systèmes informatiques au sens large présents et installés au sein de l'École Nationale Supérieur d'Architecture de Clermont-Ferrand.

La Charte Informatique a pour vocation de sensibiliser le public, ci-après désigné (cf. art 2. Périmètre utilisateur), aux exigences de sécurité et de susciter son attention sur certains comportements de nature à porter atteinte à l'intérêt collectif de l'établissement, notamment par le biais du système d'information (ci-après désigné par le « **système d'information** » ou le « **SI** »). Et éventuellement, les sanctions que l'utilisateur encourt en cas de non-respect des règles établies.

L'objectif de cette charte étant de vous donner les règles d'utilisation de l'ensemble des outils numériques. Elle vous informe de l'ensemble de droits et obligations des utilisateurs et précise les droits et obligations de l'administrateur. Vous devez vous y référer afin de prendre connaissance des sanctions applicables en cas de non-respect d'une ou plusieurs dispositions de la présente charte informatique.

Il vous engage en tant qu'utilisateur de l'outil numérique mis à disposition par l'ENSACF.

Les principes généraux qui régissent l'usage des outils informatiques :

i. **Responsabilité** : l'utilisateur est responsable des ressources informatiques mis à sa disposition, il participe au renforcement de la protection du SI en respectant les mesures décrites par la Charte.
ii. **Confidentialité** : la confidentialité est primordiale elle doit être préservée par l'utilisateur tant pour les données professionnelles et/ou universitaires que pour les données personnelles.
iii. **Respect des droits des personnes** : notamment de la vie privée, le respect des valeurs à ne pas oubliez même lorsque l'on fait usage d'outils informatiques.
iv. **Respect des intérêts de l'ENSACF** : respecter l'image de l'établissement, de ses intérêts, de son éthique.
v. **Sécurité** : mise en œuvre par un ensemble de mesures, processus mais surtout par des comportements responsables.

ARTICLE 2 : PÉRIMÈTRE UTILISATEURS

La Charte s'applique à l'ensemble des utilisateurs au sein de l'établissement, pouvant être amenés à manipuler tout moyen de communication, ressources informatiques et numériques mis à disposition par l'ENSACF.

On entend par utilisateur du SI : toute personne détentrice de manière individuelle d'une clé d'accès au Système d'Information de l'ENSACF, sans prise en compte de son statut.

On entend notamment par clé d'accès :

1. Un identificateur & un mot de passe valables ;

2. Un accès à un bâtiment ou une salle de moyens partagés ;
3. Une autorisation de connexion temporaire au réseau.

Cependant toute tierce personne amenée à manipuler les outils numériques de l'ENSACF est elle-même soumise au respect de la présente charte. Les utilisateurs s'assureront ainsi de faire respecter la Charte à toute personne, à laquelle ils permettraient l'accès du SI.

À ce titre, il est rappelé que toute intrusion non autorisée dans le SI de l'ENSACF peut être considérée comme une infraction au sens de l'article 323-1 alinéa 1 du Code Pénal.

ARTICLE 3 : PÉRIMÈTRE DU SYSTÈME D'INFORMATION

Le Système d'Information de l'ENSACF permet la constitution, la création, l'échange, la circulation, la diffusion, la duplication, la reproduction et le stockage de données, fichiers, base de données, intranet, extranet, images, sons, textes, flux d'informations entre les utilisateurs, peu importe la finalité du flux.

Le Système d'Information comprend les matériels, les logiciels et les infrastructures mis à disposition ou fournis par l'ENSACF.

Le Système d'Information est notamment composé des ressources suivantes :

- Poste de travail : ordinateur fixe / portable ;
- Salles informatiques partagées ;
- Équipements des laboratoires de recherche ;
- Réseau informatique : serveurs, routeurs et connectiques ;
- Équipement de sécurité ;
- Accès internet Réseaux : Wifi ;
- Périphériques nomades/supports amovibles : casques pc, disques durs externes, USB, etc. ;
- Périphériques : l'imprimante, scanner, etc. ;
- Services numériques : messagerie universitaire ;
- Logiciels métiers ;
- Logiciels : Pack Office, applications, etc. ;
- Serveurs fichiers & données informatisées : bases de données ;
- Téléphonie & équipement de visioconférence ;
- Appareils photo numérique & vidéo projecteurs ;
- Etc.

De plus, la Charte s'applique aussi l'ensemble des appareils connectés au Système d'Information l'ENSACF par l'utilisation des réseaux, notamment le réseau sans fil Wifi, incluant de ce fait le matériel personnel.

ARTICLE 4 : MODALITÉS DE LA CHARTE

La présente Charte est annexée au Règlement Intérieur, elle vous sera communiquée via le partage de réseau ou par voie électronique.

Le bordereau de signature, joint en fin de document, devra être remis au service de la scolarité.
Chacune des versions ultérieures de la charte informatique vous sera transmis par quelque moyen décidé par l'ENSACF : papier, sur réseau interne ou/et par courriel.

- Date création charte : 31/10/2023

- Date dernière MAJ (version) : 1.2024
- **La présente charte devient opposable au jour de : 01/09/2024**

TITRE 2 : SÉCURITÉ DU SI

La sécurité est primordiale au bon fonctionnement de l'ENSACF. L'établissement met ainsi en place les mesures nécessaires à la disponibilité, à l'intégrité mais aussi à la confidentialité et enfin à la traçabilité des données.

La disponibilité doit permettre de rendre l'information accessible lorsque l'on en a besoin. L'intégrité garantie l'exactitude de l'information afin qu'elle soit conservée de manière intacte pendant sa durée de vie. La confidentialité permet de rendre l'information accessible à un nombre limité de personnes, uniquement celles autorisées. La traçabilité est nécessaire pour avoir un suivi des accès et opérations effectuées sur l'information.

I. SÉCURITÉ PAR L'UTILISATEUR :

ARTICLE 5 : RÈGLES D'UTILISATION GÉNÉRALE

L'utilisateur est concerné par la sécurité du Système d'Information de l'ENSACF, son usage peut autant mettre à mal le système d'information que renforcer sa sécurité.

À son niveau, il contribue à la sécurité générale. Chaque utilisateur doit ainsi veiller au respect des procédures et règles de sécurité édictées par le service informatique dans le cadre de la présente Charte.
Notamment :

- Utiliser les ressources mises à disposition à des fins professionnelles, pédagogiques ou de recherche ;
- Utiliser les ressources mises à disposition à des fins privées de manière raisonnable, non lucrative, de manière à ne pas perturber le bon fonctionnement du SI et de manière limitée tant dans la fréquence que dans la durée ;
- Respecter les instructions de l'établissement quant à l'utilisation des ressources de stockages, d'impression et d'accès réseaux qui leur sont allouées.
- Respecter la législation, notamment les lois relatives aux publications et consultations à caractère illicite, injurieux, raciste, pornographique, diffamatoire ;
- Respecter les principes fondamentaux du service public de l'enseignement supérieur : égalité, laïcité & neutralité ;
- Faire un strict respect de la confidentialité.

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau qui lui sont confiées ou auxquels il a accès. Plus généralement, la sécurité est également mise en œuvre par l'utilisateur, en respectant les bonnes pratiques énoncées dans la présente charte en faisant preuve de prudence, de vigilance.

En aucun cas, l'utilisateur ne devra apporter volontairement des perturbations au bon fonctionnement du SI, que ce soit par des manipulations anormales du matériel ou par l'introduction volontaire de logiciels parasites.

ARTICLE 6 : DEVOIR D'ALERTE DE L'UTILISATEUR

Une utilisation responsable nécessite que chaque utilisateur fasse preuve de vigilance et soit impliqué par la sécurité du système d'information.

Il est demandé à chaque utilisateur de signaler à l'administrateur ou un responsable de la sécurité du système d'information de toute violation ou tentative de violation de son compte informatique, fichiers, informations ou données ou de manière générale tout dysfonctionnement ou anomalie sur du matériel.

Et ce, afin de pouvoir apprécier l'imputabilité personnelle des incidents qui pourraient survenir, mais aussi intervenir si une manipulation est nécessaire au plus vite sur le système d'information.

En cas de vol, de perte ou de dégradation de tout matériel fixe ou portable, de vol de ses supports de sauvegarde de fichiers, d'atteinte aux ressources informatiques mises à sa disposition, l'utilisateur doit en informer sans délai l'administrateur.

ARTICLE 7 : ENTRETIEN

Les utilisateurs sont tenus de verrouiller leur session lorsqu'ils quittent un poste informatique même lors d'un court instant. Cette mesure vise à empêcher qu'un autre utilisateur ou une tierce personne puisse consulter ou même utiliser votre poste sans votre accord.
Concernant les postes informatiques, il a été programmé un verrouillage automatique desdits postes après un délai de 10 minutes d'inactivité.

L'utilisateur doit éteindre son poste informatique en fin de session de travail. Il est préférable de ne pas laisser un ordinateur en veille pour préserver sa performance et économiser de l'énergie.

ARTICLE 8 : MOT DE PASSE

Le mot de passe est primordial, il demeure le premier rempart pour lutter contre les menaces, c'est pourquoi nous vous demandons d'être vigilant et responsable quant à l'usage de vos mots de passe universitaires.

L'accès aux SI ou aux ressources informatiques mises à disposition est soumis à une authentification strictement personnelle. L'authentification est composée d'un identifiant (*login*) et d'un mot de passe.

Ce mot de passe est personnel et doit le rester. Il doit être confidentiel, en aucun cas être transmis, partagé, rendu accessible à un tiers par quelque moyen que ce soit notamment.

Le mot de passe initialement attribué par l'administrateur doit être changé dès la première connexion de l'utilisateur. Ensuite, il est de la responsabilité de ce dernier de le changer selon une fréquence régulière.

Votre mot de passe ne doit pas être trivial, commun ni usuel. Il devra être composé à minima de 10 caractères incluant au minimum 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial.

En cas de trois tentatives d'authentification infructueuses au SI de l'ENSACF, le compte est bloqué 30 minutes.

Enfin, si vous suspectez une activité anormale sur vos comptes ou suspectez une authentification par un tiers à vos comptes, vous devrez changer dans les plus brefs délais votre mot passe mais aussi le signaler à l'administrateur.

Les changements de mots de passe se réalisent exclusivement à l'aide du service de cette page : https://servicepwd2.clermont-fd.archi.fr/

II. SÉCURITÉ PAR L'ENSACF :

L'ENSACF met en œuvre une série de moyens humains et techniques pour assurer la sécurité de son système d'information, des données traitées, des logiciels, des communications et en particulier des données personnelles. À ce titre elle peut limiter l'accès à certaines ressources. L'ENSACF assure la mise en œuvre et le contrôle du bon fonctionnement du SI.

ARTICLE 9 : CONTRÔLE ET TRAÇABILITÉ

Afin de garantir le bon fonctionnement de son SI, l'ENSACF se réserve le droit d'analyser, de contrôler et de filtrer les utilisations des ressources matérielles et logicielles ainsi que les échanges via les réseaux dans le strict respect de la législation en vigueur.

La responsabilité de l'ENSACF peut être engagée lors des agissements, faits, délits commis par des utilisateurs avec le matériel mis à disposition par ce dernier. Les comportements commis par négligence ou par imprudence sont y compris concernés. Ce contrôle permettra de sanctionner les éventuels abus et assurer les obligations en termes de sécurité.

L'ENSACF vous informe qu'elle enregistre les logs des logiciels métiers, que ces traces pourront être exploitées pour un contrôle. L'utilisateur peut avoir accès à ces logs, par le biais des droits d'exercice. Les logs sont conservés dans un délai de 1 an après leur enregistrement, après ce délai, ils sont automatiquement détruits.

La présente charte vous informe d'un éventuel contrôle par l'établissement des postes de travail mis à disposition.

Cependant, l'ENSACF est logiquement tenue de respecter la vie privée de chacun. L'établissement ne dérogera aucunement au secret des correspondances (sanctionné aux articles 226-15 et 432-9 du Code Pénal et par l'article L.33-1 du Code des Postes et des Communications Électroniques).

ARTICLE 10 : FILTRAGES

L'ensemble des postes de travail sont équipés d'un anti-malware composé d'un anti-virus.
L'antivirus va permettre l'identification des logiciels malveillants, les neutraliser ainsi que les effacer.

De plus, l'établissement dispose d'un pare-feu pour protéger son réseau et limiter certains trafics.

ARTICLE 11 : SAUVEGARDE(S)

Le système d'information peut être victime d'incidents tels qu'une panne matérielle, un dégât des eaux ou d'incendie, de malveillance, etc. Ces incidents peuvent être volontaires ou pas. Notamment, les données sensibles font souvent l'objet d'attaques comme les rançongiciels. Le moyen le plus sûr de s'en prémunir est d'effectuer régulièrement une sauvegarde. Les sauvegardes seront accessibles à tout moment pour pallier les différents incidents.

Chaque utilisateur est responsable de la sauvegarde de ses données. Toute autre méthode de sauvegarde non explicitement validée engage l'utilisateur y compris dans les conséquences qu'une telle action pourrait avoir sur le fonctionnement global du SI.

ARTICLE 12 : SÉCURISATION DES ACCÈS PHYSIQUES

La sécurité du système d'information de l'ENSACF passe aussi par la sécurité des accès aux locaux. A cet effet, nous vous demandons à tous d'être vigilant sur les accès physiques.

L'ENSACF a conscience de l'importance de la sécurité physique des locaux, des mesures de sécurité physique ont été mis en place afin de sécuriser l'accès.

Vous participez vous-même à la sécurité des locaux en vous assurant que les porte d'accès aux salles sont bien fermées après votre passage, il en va de même pour leur verrouillage.

TITRE 3 : SERVICES ET MATÉRIELS

ARTICLE 13 : MESSAGERIE ÉLECTRONIQUE ET OUTILS COLLABORATIFS

Votre messagerie électronique, ainsi que les outils collaboratifs rattachés à l'établissement sont des outils indispensables pour la communication en interne comme en externe. Chaque utilisateur est répertorié dans l'annuaire interne du SI et peut être associé à des listes de diffusion regroupant d'autres utilisateurs.

L'ENSACF vous fournit un compte d'accès à la messagerie et service associés, l'adresse électronique est rattachée à votre nom d'utilisateur et votre mot de passe. La messagerie électronique ne doit pas être détournée de ses fins, son accès est personnel et incessible. Vos identifiants et codes de messagerie ne doivent en aucun cas être transmis à qui que ce soit, même temporairement.

Mesures faces aux courriels suspects :

- Vous ne devez jamais ouvrir des pièces jointes de courriels dont les destinataires sont inconnus, ou dont le sujet ou le format, ou la présentation paraissent inhabituels.
- Lorsqu'un courriel contient des liens, pensez à vérifier l'adresse pointée par le lien avant de cliquer dessus, afin de vérifier la cohérence du lien.
- Ne répondez pas aux demandes d'informations personnelles, confidentielles ou bancaires par courriel, il peut s'agir de cyberattaques comme de l'hameçonnage.
- N'ouvrez pas et ne participez pas à des chaines de courriels ou des appels à solidarité, alertes virales qui semblent suspects, etc.
- Ne prenez pas de décisions importantes comme un virement par suite d'un seul courriel.
- Méfiez-vous des courriels vous demandant d'entrer vos identifiants.
- En cas de doute, merci de contacter le responsable informatique.

Fermeture de compte de messagerie et outils collaboratifs :

Toute fermeture de compte de messagerie et outils collaboratifs associés entraîne la suppression des données de l'utilisateur du SI de l'école.

ARTICLE 14 : NAVIGATION INTERNET

La connexion internet vous est mise à disposition dans le cadre de fins universitaires.

Dans le cadre de ces fins, il est conseillé d'utiliser la connexion fournie et sécurisée de l'ENSACF.

L'établissement dispose un droit de regard, qui peut se manifester par un éventuel contrôle.

Nous vous rappelons que la connexion internet ne doit pas permettre la commission d'actes qui porteraient atteinte aux intérêts de l'ENSACF (ni à la réputation ni au système d'information, ni à la confidentialité des données), ou un usage prohibé (comme le téléchargement illégal ou l'envoi de message portant atteinte à la dignité humaine, ni permettre la commission d'actes illicites).

La navigation internet offre de nombreuses facilités, vous devez pour autant gardez en tête que l'utilisation de cet accès doit rester loyale et rationnelle.

Pour des raisons de sécurité, l'accès à certains sites est limité ou prohibé par l'ENSACF. A ce titre, nous mettons en place un dispositif de filtrage des sites prohibés par le blocage d'accès à une liste d'URL. À noter que cette mesure ne constitue pas en soi une atteinte à la vie privée.

De plus, un contrôle physique des historiques de navigation aux horaires de travail pourra être mis en place afin de prévenir les abus. Cet éventuel contrôle n'a pas vocation à porter atteinte à la vie privée et pourra se faire en l'absence de l'utilisateur.

À ce titre, il est notamment interdit d'accéder à :

- Sites dont le contenu est contraire à l'ordre public et aux bonnes mœurs ;
- Sites pouvant comporter un risque pour la sécurité du SI ;
- Sites à caractère pornographique & pédophile ;
- Sites de jeux en ligne, et notamment des sites de jeux d'argent ;
- Sites racistes, négationnistes & révisionnistes ;
- Sites portant atteinte à la dignité humaine ;
- Sites de terrorisme ;
- Sites illicites (drogue, vente d'arme, etc.) ou contraire à la loi ou contraire à l'éthique de notre établissement ;

De plus, il est fortement déconseillé d'inscrire votre adresse de messagerie universitaire sur des sites afin de limiter la réception de mails indésirables.

La connexion internet est sécurisée par un antivirus ainsi qu'un pare-feu et pourra limiter l'accès à certains sites.

Vous devez être vigilant lors de votre navigation internet, et privilégier les sites web présentant un cadenas et la mention *https*.

La navigation internet est souvent la cible des cyberattaques, il vous est demandé d'être prudent. En cas de doute ou de problème, merci de contacter le responsable informatique.

ARTICLE 15 : RÉSEAUX SOCIAUX

Vous ne devez en aucun cas nuire à l'ENSACF ou à sa réputation en lui causant du tort de quelque manière que ce soit, notamment en divulguant des informations confidentielles.

Tout utilisateur se doit de respecter la vie privée des tiers en ne communiquant aucune information personnelle sans son accord (identité, adresse électronique, numéro de téléphone, adresse postale, situation familiale, etc.).

Les pages des réseaux sociaux de l'ENSACF ont pour objectif de développer une communauté internet amicale autour de notre entité et de son actualité afin d'échanger des opinions et des idées.

En utilisant ces différentes pages, vous vous engagez à publier des contenus respectant les lois et règlements en vigueur, n'étant pas contraire à l'ordre public ou aux bonnes mœurs, et ne portant pas atteinte aux droits des personnes.

Même si les réseaux sociaux appellent à un langage plus familier, aucun contenu injurieux, grossier, vulgaire ou de nature à heurter la sensibilité des personnes ne sera accepté.

Les administrateurs des réseaux sociaux de l'ENSACF se réservent donc le droit de supprimer tout contenu inopportun, notamment : racistes, xénophobes, pornographiques, diffamatoires, injurieux, dénigrants,

insultants, discriminatoires, haineux, agressifs, choquants ou violents, discréditant autrui, publicitaires, portant atteinte à l'image d'une personne ou au respect de sa vie privée, etc.

En tout état de cause, chaque situation considérée comme abusive pourra faire l'objet de sanction disciplinaire, de poursuite civile ou pénale selon la gravité de l'abus, qu'elle ait eu lieu sur un réseau social rattaché à l'ENSACF ou personnel à l'utilisateur.

ARTICLE 16 : LOGICIELS

L'ENSACF vous met à disposition des logiciels. Ces logiciels respectent les droits de propriété, ils sont sous licence. Il est interdit de porter atteinte au droit de la propriété intellectuelle de ces logiciels, vous ne devez pas les reproduire ni les modifier.

Il est formellement interdit de ; télécharger, implémenter, utiliser en ligne, etc. des logiciels autres que ceux fournis par l'ENSACF au sein de son SI sans autorisation, notamment si ces derniers sont dits « piratés ». À défaut, votre responsabilité pourra être engagée à titre individuel.

ARTICLE 17 : SUPPORTS AMOVIBLES

Les supports amovibles comme des clés USB, des disques durs externes peuvent être utilisés de manière récurrente pour transporter des données facilement, de poste à poste.

Ces supports peuvent être compromis par un logiciel malveillant, puis agir sur le poste de travail ou même sur le réseau. Les supports amovibles peuvent se perdre facilement sans sécurité ; la confidentialité des informations, données sensibles est rompue, un tiers peut y accéder et en faire ce qu'il veut.

À ce titre, l'usage, l'échange et le prêt d'un support amovible doivent faire l'objet d'une attention toute particulière.

TITRE 4 : CADRE JURIDIQUE

ARTICLE 18 : HARCELEMENT

L'outil numérique facilite la communication, la liberté d'expression. Attention il ne faut pas en abuser.

Les propos publiés sur les forums, conversations, publications sur les réseaux sociaux, échangés par courriel qui porteraient atteinte à la l'établissement ou aux droits des personnes, peuvent être constitutifs d'une faute grave susceptible de justifier une sanction.

Le harcèlement peut se manifester par des remarques négatives, des critiques ou des sarcasmes répétés, de l'intimidation, des menaces, des insinuations, des humiliations, des abus de droit, la circulation de fausses informations concernant la personne, des tentatives pour isoler socialement la victime. L'auteur de ce comportement encourt des poursuites à son encontre.

À ce titre, un utilisateur qui serait victime ou témoin d'harcèlement doit se tourner auprès de l'interlocuteur référent au sein de l'ENSACF : Amélie FLAMAND (amelie.flamand@clermont-fd.archi.fr).

ARTICLE 19 : PROTECTION DES DONNÉES PERSONNELLES

L'ENSACF veille au respect de la réglementation sur la protection des données à caractère personnel notamment :

1. La loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (loi Informatique et Libertés) ;
2. Le règlement général n◦ 2016/679 relatif à la protection des données à caractère personnel (RGPD) du 27 avril 2016, promulgué le 25 mai 2018.

Vous disposez d'un droit d'accès et de rectification, droit de limitation, droit d'opposition en cas de raisons légitimes. Si vous souhaitez adresser votre demande d'exercice des droits, ou souhaitez poser une question sur l'exercice des droits, contactez le délégué à la protection des données personnelles de l'ENSACF par voie électronique : DELMARE Hervé (herve.delmare@culture.gouv.fr).

Si vous estimez, après nous avoir contactés, que vos droits « Informatique et Libertés » ne sont pas respectés, **vous disposez du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).**

ARTICLE 20 : PROPRIÉTÉ INTELLECTUELLE

La présentation et le contenu des ressources numériques de l'ENSACF constituent une œuvre protégée par les lois en vigueur sur la propriété intellectuelle.

Aucune exploitation commerciale, reproduction, représentation, utilisation, adaptation, modification, incorporation, traduction, commercialisation ; partielle ou intégrale des éléments des ressources ne pourra en être faite sans l'accord préalable de l'établissement et des auteurs.

L'utilisateur est responsable, en tous lieux, de l'usage qu'il fait du système d'information auquel il a accès et plus particulièrement des supports, tous formats numériques confondus, mis à disposition dans le cadre de sa formation.

Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Tous les supports audiovisuels sont mis à disposition pour l'année universitaire et sont réservés à un usage personnel. Ces supports ne doivent en aucun cas être dupliqués ou diffusés.

ARTICLE 21 : SANCTIONS APPLICABLES

Le manquement aux règles et mesures de sécurité de la présente Charte est susceptible d'engager la responsabilité de l'utilisateur.

Tout manquement pourra faire l'objet d'avertissement, de limitations mais aussi de suspensions du système d'information.

Les sanctions disciplinaires s'appliqueront et seront proportionnées selon la gravité des faits concernés conformément au Règlement Intérieur.

L'ENSACF se réserve le droit d'engager des poursuites civiles et pénales devant les juridictions compétentes indépendamment des sanctions disciplinaires engagées.

ANNEXE n°1 : RÉGLEMENTATION EN VIGUEUR

- Règlement intérieur ;
- Règlement général sur la protection des données à caractère personnel (RGPD) ;
- Loi informatique et libertés (LIL) ;
- Code Civil :
    - Article 1104 (bonne foi exécution des contrats)
    - Etc.
- Code Pénal :
    - Articles 226-1 et suivants (protection de la vie privée)
    - Article 227-23 et suivants (accès aux sites pornographiques)
    - Article 323-1 et suivants (atteinte STAD)
    - Article 222-33-2 (harcèlement moral)
    - Article 314-1 (abus de confiance)
    - etc.
- Code de la Propriété Intellectuelle ;
- Loi HADOPI.

BORDEREAU DE SIGNATURE

CHARTE INFORMATIQUE ENSACF VERSION 1.2024

Je, soussigné(e) reconnais avoir pris connaissance de la charte informatique de l'ENSACF et, à ce titre, m'engage en qualité d'utilisateur du SI à :

1. Utiliser les ressources mises à ma disposition selon des fins adéquates ;
2. Utiliser les ressources mises à ma disposition de manières raisonnable, ne perturbant pas le bon fonctionnement du SI ;
3. Respecter les législations et réglementations en vigueur ;
4. Respecter les principes fondamentaux du service public de l'enseignement supérieur ;
5. Faire un strict respect de la confidentialité ;
6. Faire preuve de vigilance et signaler toute violation ou tentative de violation d'une ressource ainsi que tout dysfonctionnement ou anomalie ;
7. D'entretenir correctement le matériel mis à ma disposition ;
8. Maintenir la confidentialité de mes mots de passe personnels ;
9. Faire un usage adéquat de ma messagerie électronique, de la navigation internet & des réseaux sociaux ;
10. Ne pas porter atteinte aux droits de propriété intellectuelle ;

Fait à …… Le / / 20……

SIGNATURE

Remettre le bordereau de signature de la charte informatique auprès du Service de la scolarité. Pour toutes questions ou remarques : Direction des Systèmes d'Information.