CHARTE INFORMATIQUE

PREAMBULE

Horizon University met à disposition de ses utilisateurs un système d'information (SI) et des moyens informatiques nécessaires à l'exécution de ses missions et de ses activités. Dans le cadre de leurs fonctions, les utilisateurs sont conduits à utiliser ces ressources informatiques.

Celles-ci comprennent :

- Des réseaux informatiques
- Des réseaux téléphoniques
- Des systèmes d'informations
- Des contenus pédagogiques
- Des comptes emails
- Des ressources Cloud

Dans un objectif de transparence, la présente charte définit les règles dans lesquelles ces ressources peuvent être utilisées.

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs des ressources informatiques dont notamment :

- Les étudiants
- Les enseignants permanents
- Les enseignants contractuels
- Les enseignants vacataires et experts
- Les employés administratifs
- Les visiteurs occasionnels

Il appartient aux responsables et enseignants d'Horizon University de s'assurer de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès aux ressources informatiques.

Article 2 : Périmètre du système d'information

Les systèmes d'information sont composés des ressources suivantes :

- Ordinateurs

- Téléphones
- Réseau informatique (serveurs, routeurs et connectique)
- Photocopieurs
- Logiciels
- Données informatisées
- Email et messagerie
- Ressources Cloud

Aux fins d'assurer la sécurité informatique des SI, tout matériel connecté aux SI de l'entreprise, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente charte.

Article 3 : Règles générales d'utilisation

Les SI doivent être utilisés à des fins professionnelles, conformes aux objectifs de l'université (enseignement, formation, recherche scientifique, etc.), sauf exception prévue par les présentes, ou par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser les SI de l'université pour se livrer à des activités concurrentes, et/ou susceptibles de porter préjudice à l'université ou autrui de quelque manière que ce soit.

Article 4 : sécurité informatique

Horizon University met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles. A ce titre, elle peut limiter l'accès à certaines ressources.

4.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

4.1 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

4.2 Mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le

contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

4.3 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

4.4 Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

4.5 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (vol de clé USB, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles, etc.).

Article 5 : Accès à Internet

L'accès à l'Internet est autorisé au travers des SI, toutefois, pour des raisons de sécurité l'accès à certains sites peut être limité. L'utilisateur doit respecter les droits d'exploitation et d'utilisation des ressources et des données en naviguant sur Internet via les SI. Aucun téléchargement contraire à ces lois n'est permis.

Article 7 : Email

Chaque utilisateur (étudiants, enseignants permanents, administratifs) peut disposer d'une adresse email pour l'exercice de ses missions.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi.

Il est interdit d'entrer dans aucune activité de SPAM ou d'envoie illégale d'email pour n'importe quelle raison.

Article 8 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du SI, sanctions disciplinaires, etc).

Article 9 : Information et entrée en vigueur

La présente charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque utilisateur.

Elle entre en vigueur dès la date de sa signature par l'intéressé(e).

Sousse, le ……..

Nom et Prénom : ……

Signature (précédée par la mention « lu et approuvé »)