Charte d'utilisation des ressources informatiques et du système d'information de l'Université Saint-Joseph de Beyrouth

(Texte approuvé par le Conseil de l'Université lors de sa 200ème réunion en date du 19 juin 2019)

Introduction

La présente Charte définit les règles d'utilisation des ressources informatiques et du système d'information de l'Université Saint-Joseph de Beyrouth (ci-après : l'Université). Elle précise les obligations respectives des utilisateurs et de l'Université. Elle vaut pour tous les ordinateurs, qu'ils soient fixes ou nomades, collectifs ou personnels.

Son objet est aussi de sensibiliser les utilisateurs aux risques liés à l'utilisation des ressources informatiques, notamment en ce qui concerne la confidentialité des données. Elle incite toutes les personnes intéressées à la prudence dans le maniement de ces ressources. Elle rappelle en particulier que l'utilisation de l'informatique doit se concilier avec les droits de propriété intellectuelle.

Les ressources informatiques dont il s'agit sont celles que l'Université met à disposition des utilisateurs dans le cadre de leur activité professionnelle. Ces ressources comprennent notamment le système d'information, c'est-à-dire tous les moyens matériels, logiciels, bases de données ou réseaux de télécommunications mis à la disposition des utilisateurs.

Cette mise à disposition doit être pleinement respectueuses des libertés collectives et individuelles. Elle préserve en particulier la vie privée, les données à caractère personnel et la propriété. Elle se conforme par ailleurs à la législation libanaise, ainsi qu'aux règlements de l'Université Saint-Joseph de Beyrouth.

La présente Charte, ainsi que toute modification ultérieure, entre en vigueur à dater de son adoption par le Conseil de l'Université.

Tout utilisateur des ressources informatiques et du système d'information de l'Université devra être avisé de cette Charte et la signer.

1. Obligations de l'utilisateur

1.1. Obligations générales

Outre les obligations liées à son statut ou à son contrat, pèsent sur l'utilisateur les obligations générales suivantes :

1.1.1. L'utilisateur est responsable de l'usage qu'il fait des ressources informatiques et du système d'information de l'Université.

1.1.2. Il lui est interdit de propager des messages haineux ou diffamatoires, ou toute forme d'apologie de crime, de racisme, etc.

1.1.3. Il ne peut reproduire, diffuser ou modifier les logiciels, bases de données, pages web, textes, photographies, ou toute autre création protégée par le droit d'auteur, qu'avec l'accord du titulaire du droit. L'utilisateur doit respecter également le droit des marques.

1.1.4. Il a une obligation de réserve et de confidentialité à l'égard des correspondances, des informations et des documents auxquels il peut avoir accès.

1.1.5. À son départ définitif de l'Université, l'utilisateur perd son droit d'accès aux ressources informatiques, notamment au WiFi, et au système d'information.

L'Université peut toutefois lui conserver son adresse électronique (@usj.edu.lb ou @net.usj.edu.lb) ; l'utilisateur s'engage alors à respecter, même après son départ, la présente Charte.

1.2. Obligations spéciales

1.2.1. Obligations liées au caractère professionnel des activités de l'utilisateur

Les services informatiques de l'USJ sont réservés à des activités professionnelles, c'est-à-dire à celles qui sont liées à l'enseignement, à la recherche, à l'administration de l'Université et au fonctionnement des services de celle-ci.

a. L'utilisateur doit garantir l'accès à tout moment, même en son absence, à ses données professionnelles lorsqu'elles sont liées à l'administration de l'Université et au fonctionnement des services de celle-ci.

   Les conditions d'accès aux données professionnelles liées aux activités de recherche collective sont déterminées par les laboratoires et les centres de recherche concernés.

b. De manière occasionnelle, l'utilisateur peut faire un usage privé de son poste de travail, à la condition qu'il n'ait aucune finalité lucrative. L'utilisateur est par ailleurs seul responsable des données à caractère privé le concernant sauvegardées sur son poste de travail ; il doit les supprimer à son départ, faute de quoi l'Université se réserve le droit de le faire.

c. S'il utilise les réseaux sociaux à partir des ressources informatiques de l'Université, l'utilisateur doit se conformer à la *Charte d'utilisation des réseaux sociaux de l'Université Saint-Joseph de Beyrouth*.

1.2.2. Obligations liées à la sécurité informatique

Dans un but de sécurité, l'utilisateur doit :

a. Verrouiller, à l'issue de son utilisation, le poste de travail personnel ou collectif dont il s'est servi.

b. S'abstenir de divulguer ses mots de passe aux tiers, y compris à son supérieur hiérarchique, sauf motifs impérieux.

c. S'abstenir de télécharger ou d'installer, sur son poste de travail professionnel, des logiciels ou des progiciels gratuits ou payants, sauf autorisation expresse de l'Université.

d. Utiliser les outils et les moyens de sauvegarde des données que l'Université met à sa disposition. L'utilisateur ne dépose pas des données sur un serveur ouvert au grand public (Google, Yahoo, …) sans y être autorisé par les responsables habilités.

e. S'abstenir de retirer des données à caractère professionnel et de les utiliser, en dehors des locaux de l'Université, sans autorisation préalable.

f. Avertir son supérieur hiérarchique ou le Responsable de la sécurité des systèmes d'information de toute tentative de violation de son compte ou de toute autre anomalie.

g. Se conformer aux dispositifs prévus par l'Université pour lutter contre les virus et les attaques informatiques.

h. Les visiteurs de l'Université ne peuvent avoir accès au Système d'information qu'avec l'accord préalable de l'administrateur des ressources informatiques.

2. Obligations de l'Université

2.1. Obligations générales

2.1.1. L'Université garantit le bon fonctionnement et la sécurité des réseaux. Elle assure cette mission dans le respect de la législation et des réglementations en vigueur, notamment celles relatives à la protection des données à caractère personnel et au respect de la vie privée.

2.1.2. Elle porte à la connaissance de tout intéressé sa politique de sécurité, ainsi que les règles de bon usage des ressources informatiques et du système d'information.

2.1.3. Elle organise des sessions d'information et de formation à l'utilisation des ressources informatiques.

2.1.4. Elle fournit à tout utilisateur un « authentifiant et mot de passe », qui lui est personnel.

2.1.5. La nécessité d'assurer la sécurité du réseau peut engendrer des interventions de l'Université sur le poste de l'utilisateur. Ces interventions sont précédées d'une prise de contact avec l'intéressé qui doit en être informé.

2.1.6. L'administration et la maintenance des réseaux informatiques peut donner lieu à des collectes statistiques nécessitant le référencement des utilisateurs. Ces derniers en seront préalablement informés par l'Université. Les personnels qui ont la charge de la collecte sont soumis au secret professionnel.

2.1.7. L'Université désigne un ou plusieurs administrateurs des ressources informatiques et du système d'information.

2.2. Obligations de l'administrateur

Outre les obligations qui s'imposent à tout utilisateur, l'administrateur est également soumis aux obligations suivantes :

2.2.1. Il fournit aux utilisateurs l'accès aux ressources informatiques et aux modules du système d'information et veille à leur bon fonctionnement.

2.2.2. Il respecte les droits de l'utilisateur, en particulier ses libertés individuelles et sa vie privée.

2.2.3. Il préserve la confidentialité des données dont il dispose, en particulier celles de nature privée ou confidentielle qu'il serait amené à connaître dans le cadre de son activité.

2.2.4. Il se conforme aux règles de l'éthique professionnelle et de la déontologie.

2.2.5. Il constitue des archives de sorte à préserver la continuité du service à son départ définitif de l'Université.

2.2.6. L'administrateur veille à garantir la sécurité informatique. À cette fin, il doit :

a. S'assurer du respect des consignes de sécurité par les utilisateurs.

b. Filtrer ou interdire l'accès à certains sites, ainsi qu'au téléchargement de fichiers, s'ils présentent un risque avéré pour le système d'information de l'Université.

c. Agir au plus tôt lorsqu'il a connaissance d'actions illégales ou de données illicites sur les équipements informatiques.

d. Avertir sans délai son supérieur hiérarchique et le Responsable de la sécurité des systèmes d'information de tout incident de sécurité, anomalie, vulnérabilité ou dysfonctionnement.

e. Garder strictement confidentiel son propre mot de passe, sauf impératif lié à la nécessité d'assurer la continuité de son service et de sa mission.

f. Effectuer à échéance régulière un audit de tous les accès aux ressources informatiques et au système d'information de l'Université. Cet audit doit permettre de déceler les tentatives de violation du système informatique et aider à déterminer les responsabilités éventuelles.

g. Les actions de maintenance ou de suivi des ressources informatiques impliquent le cas échéant que l'administrateur accède à l'ensemble des données des utilisateurs. En ce cas, il est pleinement soumis au devoir de confidentialité absolue. Il respecte par ailleurs la propriété privée.

3. Sanctions

Sans préjudice des procédures disciplinaires ou judiciaires susceptibles d'être engagées à l'encontre des contrevenants, l'Université pourra suspendre l'accès aux ressources informatiques et au système d'information pour tout utilisateur qui méconnaitrait les dispositions de la présente Charte.

Annexe à la Charte d'utilisation des ressources informatiques et du système d'information de l'Université Saint-Joseph de Beyrouth

Définitions

Administrateur : Tout personne, membre du personnel du Service de technologie de l'information (STI), chargé explicitement du développement, de l'exploitation, de la maintenance et du suivi de l'utilisation des ressources informatiques et du système d'information de l'Université et disposant, à ce titre, de droits d'accès spécifiques et privilégiés. Dans le cadre de son activité, l'Administrateur pourrait être amené à avoir accès aux informations des autres utilisateurs ou relatives à leurs activités, ainsi qu'à des sources d'informations confidentielles.

Appareils nomades : Les équipements mobiles qui permettent l'accès à distance aux ressources informatiques de l'Université, notamment les téléphones portables, les tablettes, les ordinateurs portables.

Données : Toute information disponible sous différents formats (base de données, fichiers, documents imprimés, courriers électroniques, etc.)

Politique de sécurité : Ensemble des directives et procédures ayant pour objectif la protection des ressources informatiques et du système d'information de l'Université.

Ressources informatiques : L'ensemble des moyens matériels et des outils informatiques ou numériques qui peuvent être mis à la disposition des utilisateurs dans le cadre de leur activité professionnelle.

Sécurité du système d'information : ensemble des moyens techniques, organisationnels, juridiques et humains mis en place pour conserver et garantir la sécurité des ressources informatique et du système d'information.

Système d'information : Ensemble de modules informatiques intégrés servant comme outil de gestion de l'Université.

Utilisateur : toute personne, quel qu'en soit le statut, qui a accès de manière continue ou occasionnelle dans le cadre de son activité professionnelle, par le biais d'appareils fixes ou nomades, aux ressources informatiques ou au système d'information de l'Université. Sont utilisateurs :

- Tout membre du personnel des services généraux, cadré ou non-cadré ;
- Tout enseignant, cadré ou non-cadré ;
- Tout étudiant ou stagiaire ;
- Tout chercheur ou doctorant ;
- Tout invité de l'Université ;
- Tout prestataire ayant contracté avec l'Université ;
- Tout administrateur ;
- Et plus généralement l'ensemble des personnes utilisant les ressources informatiques de l'Université, ainsi que celles accessibles à distance à partir du réseau de l'Université.

Dispositions applicables

- Le préambule de la Constitution Libanaise du 21/9/1990 relatif au respect de la vie privée.
- La loi no. 75 du 3 avril 1991 relative au respect de la propriété intellectuelle.
- La loi no. 81 du 10 octobre 2018 relative aux transactions électroniques.
- La loi no. 29 du 10 février 2017 relative au droit d'accès à l'information.
- Dispositions pénales : art. 579 et s. du Code pénal libanais.
- Charte des réseaux sociaux de l'Université Saint-Joseph de Beyrouth.

Nom .....

Prénom .....

Fonction .....

Institution .....

Lu et approuvé (Signature) .....

Date .....