Charte pour l'utilisation des ressources informatiques de l'Université Claude-Bernard Lyon1

Approuvée par délibération du Conseil d'Administration de l'UCBL en séance du 19 décembre 2017

Vu le code de l'éducation ;
Vu le code de la propriété intellectuelle ;
Vu le code pénal ;
Vu l'avis favorable du conseil académique en date du 16 novembre 2017 ;
Vu l'avis favorable du comité technique en date du 15 décembre 2017 ;

PREAMBULE

La présente Charte est une annexe du règlement intérieur de l'UCBL et a la même force obligatoire. Elle définit les règles relatives à l'utilisation du système informatique (SI) de l'université et tend à sensibiliser les utilisateur·trices aux risques liés à son utilisation en termes d'intégrité et de confidentialité des données traitées et de sécurité informatique.

Elle s'appuie sur 10 principes fondamentaux :

1. Le mot de passe d'un compte informatique est strictement personnel et confidentiel.
2. Les moyens informatiques sont mis à disposition des utilisateurs à des fins professionnelles.
3. L'utilisateur·trice est responsable de l'usage qu'il·elle fait du SI et s'engage à ne pas apporter volontairement de perturbations à son fonctionnement.
4. L'utilisateur·trice doit protéger et sauvegarder son poste de travail.
5. L'utilisateur·trice doit respecter la propriété intellectuelle, les contenus à caractère confidentiel et la vie privée.
6. L'utilisateur·trice ne doit pas utiliser le SI :
    - pour harceler d'autres utilisateur·trices ;
    - pour diffuser des informations fausses, illégales, diffamatoires ou à caractère discriminatoire ;

   En toutes circonstances, les utilisateur·trices doivent respecter les principes fondamentaux du service public de l'enseignement supérieur (égalité, laïcité, neutralité notamment commerciale).
7. Dans un cadre professionnel, l'utilisateur·trice doit utiliser les services numériques mis à disposition par l'université.
8. Les données dont le caractère privé n'est pas expressément mentionné sont réputées à caractère professionnel.
9. Le·la responsable du système d'information de l'université (RSSI) et les administrateur·trices du SI ont accès à l'ensemble des données techniques pour assurer leurs missions mais s'engagent à respecter les règles de confidentialité.
10. Tout manquement aux règles de la présente Charte est susceptible d'engager la responsabilité de l'utilisateur·trice.

Les utilisateur·trices doivent également se conformer à la charte RENATER[1] (le réseau de l'UCBL étant raccordé à Internet via le réseau national RENATER) et à la Politique de Sécurité du Système d'Information[2] (PSSI) de l'Université.

[1] https://www.renater.fr/IMG/pdf/charte_fr.pdf
[2] http://intranet.univ-lyon1.fr/medias/fichier/pssi-ucb-lyon-1-validee-_1392384586541-pdf

Article 1er Champ d'application et définitions

1.1 Périmètre

On entend par système d'information (SI) l'ensemble des moyens mis en œuvre par l'établissement pour opérer les services nécessaires à ses missions et qui traitent les informations de Gestion, d'Enseignement et de Recherche.

Les moyens sont :

- Les matériels informatiques
- Les logiciels
- Les données
- Les personnes
- Les infrastructures
- Le réseau

La présente Charte s'applique :

- à tous les métiers de l'université
- à tous ses sites et locaux
- à tous les utilisateur·trices de son SI, y compris les étudiant·es, stagiaires, auditeur·trices
- à tous les supports de l'information
- à tous les types d'accès

1.2 Utilisateurs

On entend par utilisateur·trice : les personnes titulaires d'un compte d'accès (personne physique ou morale, interne ou externe). Les intervenants extérieurs doivent respecter et faire respecter la présente Charte par leurs propres personnels et éventuels sous-traitants.

Les accès sont attribués :

- aux personnels et assimilés dès que leur dossier présente une date d'affectation valide dans le système d'information RH ;
- aux étudiant·es dès que leur inscription administrative est terminée ;
- aux prestataires lorsque leur dossier est enregistré dans le SI des prestataires.

L'accès est retiré trois mois après la date à laquelle ils perdent la qualité au titre de laquelle l'accès leur a été attribué. Toutes les données à caractère privé sont supprimées à l'issue de ce délai, il appartient alors à chaque utilisateur·trice préalablement au retrait de son droit d'accès de sauvegarder son espace de données à caractère privé.

1.3 Compte d'accès pour certains éléments du système d'information

Confidentialité : L'accès au SI repose sur l'utilisation d'un nom de compte (identifiant) fourni à l'utilisateur·trice lors de son arrivée à l'Université et d'un mot de passe créé par l'utilisateur·trice à son arrivée et qui doit rester strictement confidentiel.

Avant la première connexion, l'utilisateur·trice doit activer son compte en fournissant plusieurs informations confidentielles contenues dans le SI de LYON 1 (Nom, prénom, date de naissance, et numéro de dossier HARPEGE ou numéro INE3) à l'aide d'un formulaire en ligne. Une fois le formulaire d'activation rempli, l'utilisateur·trice est redirigé·e vers un second formulaire de saisie de mot de passe qui exigera un mot de passe suffisamment complexe et conforme aux recommandations en matière de sécurité des systèmes d'information.

Les utilisateur·trices ne doivent pas stocker leurs mots de passe en clair (dans un mail, un fichier ou sur un papier).

L'utilisateur·trice ne doit pas divulguer ou s'approprier les identifiants d'un·e autre utilisateur·trice.

Identification : L'identification de l'utilisateur·trice est obligatoire, y compris pour l'accès au réseau. Les informations qu'il donne doivent être exactes et actuelles.

[3] Le numéro de dossier HARPEGE et le numéro INE sont des informations confidentielles qui ne peuvent être communiquées sans s'assurer de l'identité de la personne.

L'utilisateur·trice est responsable des opérations effectuées grâce à son identifiant et son mot de passe, notamment en cas de manquement de sa part aux obligations de sécurité.
L'utilisateur·trice est responsable de l'utilisation des ressources informatiques (locales ou distantes) effectuée à partir de son droit d'accès.
Le droit d'accès aux SI est temporaire ; il peut être suspendu ou retiré en cas de risque immédiat pour le SI ou de non-respect de la présente Charte (cf. article 5 Sanctions).

Article 2 Obligations de l'utilisateur·trice

2.1 Obligations générales de l'utilisateur·trice

2.1.1 Utilisation conforme aux missions de l'université

Les moyens informatiques sont mis à disposition des utilisateur·trices à des fins professionnelles en ce qui concerne les personnels ou assimilés et à des fins liées à la pédagogie, à la recherche, à l'orientation ou à l'insertion professionnelle en ce qui concerne les étudiant·es.
L'utilisation à des fins privées est tolérée sous réserve qu'elle soit non lucrative, raisonnable, qu'elle ne perturbe pas le fonctionnement du SI et limitée tant dans la fréquence que dans la durée. Elle doit être conforme à la loi, à l'ordre public et à la Charte RENATER.
Il est fortement recommandé à l'utilisateur·trice de ne pas :

- utiliser son adresse professionnelle pour s'inscrire sur des sites à usage non professionnel (ex : réseaux sociaux, sites commerciaux etc.) ;
- stocker des fichiers personnels (ex : photos de vacances, films, musique etc.).

En toutes circonstances, les utilisateur·trices doivent respecter les principes fondamentaux du service public de l'enseignement supérieur (égalité, laïcité, neutralité notamment commerciale).

2.1.2 Obligations générales de sécurité

L'utilisateur·trice doit informer immédiatement l'administrateur de toute perte, de toute tentative de violation ou anomalie relative à une utilisation de son compte d'accès et de manière générale de tout dysfonctionnement.
L'utilisateur·trice est responsable de l'usage qu'il·elle fait du SI. Il assure notamment, à son niveau, la sécurité de ce SI et s'engage à ne pas apporter volontairement de perturbations à son fonctionnement et à mettre en péril l'intégrité des ressources. L'utilisateur·trice respecte notamment les règles suivantes :

- ne pas interrompre le fonctionnement normal du réseau ou des systèmes connectés ;
- ne pas développer, installer ou copier des programmes destinés à contourner la sécurité, saturer les ressources ;
- ne pas introduire de logiciels malveillants ou programmes contournant la protection des logiciels ne pas installer de logiciels susceptibles de modifier la configuration des outils sans accord préalable de l'administrateur;
- ne pas s'attaquer au SI de l'université ou de tout autre organisme, en modifier ou altérer le contenu ;
- ne pas collecter ou tenter de collecter des informations susceptibles d'être utilisées lors de tentatives d'attaques contre des systèmes d'information externes ou internes ;
- n'entreprendre aucune action qui constitue un trouble à l'ordre public ou un manquement aux droits de tiers.

2.2 Obligations relatives au poste de travail

L'utilisateur·trice respecte notamment les règles suivantes :

- Maintien d'un « poste propre » : système d'exploitation et antivirus à jour, pare-feu activé pour les versions de système qui le permettent, pas d'installation de logiciels illégaux ou destinés à contourner la sécurité.
- Toutes données stockées sur un poste de travail nomade se trouvent également exposées ; il revient à l'utilisateur·trice d'en assurer la sauvegarde et/ou le chiffrement si la sensibilité ou la confidentialité le justifie.
- Verrouillage du poste : activation du verrouillage automatique de session en cas d'inactivité du poste.

2.3 Obligations relatives aux données

2.3.1 Respect du caractère confidentiel des informations

L'utilisateur·trice respecte les contenus à caractère confidentiel, et s'engage particulièrement dans ce cas :

- à ne pas lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur·trice sans y avoir été explicitement autorisé·e par son propriétaire et/ou son auteur ;
- à ne pas intercepter, détourner, utiliser ou divulguer les communications entre tiers ;
- à suivre le principe du moindre privilège : chaque utilisateur·trice ne doit posséder que les privilèges et ressources nécessaires à ses missions et rien de plus.

2.3.2 Respect de la propriété intellectuelle

Les utilisateur·trices doivent s'abstenir de copier, diffuser ou reproduire tout logiciel ou document protégé par le droit d'auteur. Ils utilisent les logiciels et données conformément aux licences souscrites.

De manière générale, les utilisateur·trices s'assurent que les données qu'ils diffusent sur Internet ou qu'ils téléchargent ne portent pas atteinte aux droits des tiers (droit d'auteur, droit des marques, droit au respect de la vie privée etc.).

2.3.3 Respect du droit des personnes

Il est interdit à tout utilisateur·trice de porter atteinte à la vie privée d'autrui par un procédé quelconque et notamment par la transmission sans son consentement de son image ou de ses écrits diffusés à titre confidentiel ou privé. De manière générale, l'utilisateur·trice veille au respect de la personnalité, de l'intimité et de la vie privée d'autrui.

2.3.4 Respect des clauses contractuelles

Les utilisateur·trices doivent respecter les conditions contractuelles prévues notamment pour l'usage des ressources documentaires électroniques et en avoir un usage raisonnable, personnel et strictement non commercial.

2.3.5 Respect d'un comportement correct

Un utilisateur·trice ne doit pas utiliser le SI pour harceler d'autres utilisateur·trices par des communications non souhaitées par les tiers ou pour afficher/diffuser des informations fausse ou illégales.

Il est également interdit de consulter, charger, stocker, diffuser *via* les moyens informatiques des documents, informations, images, fichiers… contraires à la loi ou à l'ordre public et plus particulièrement à caractère violent, pornographique, incitant au racisme ou à la violence, portant atteinte au respect de la personne humaine et de sa dignité ainsi qu'à la protection des mineurs ; de caractère diffamatoire ou injurieux et de manière générale illicite.

2.3.6 Respect de la déontologie informatique

Les utilisateur·trices ne doivent pas effectuer de manœuvres qui auraient pour objet de méprendre les autres utilisateur·trices sur leur identité.

Les utilisateur·trices doivent respecter les procédures d'authentification en vigueur de façon à ce que les actions qu'ils mènent au sein des systèmes soient identifiables

2.3.7 Responsabilité des utilisateur·trices en tant qu'auteurs de contenus

Les utilisateur·trices qui mettent en ligne des contenus illicites, quel que soit le support utilisé (sites webs, pages personnelles, forum, wiki, messages etc.) sont responsables civilement et pénalement.

2.4 Externalisation

Dans un cadre professionnel, les personnels et les doctorant·es de l'université doivent utiliser les services numériques mis à disposition par l'université (mail, partage de fichier, plateforme de travail collaboratif …) et non des outils fournis par un prestataire extérieur (gratuit ou non) qui peuvent exposer de façon incontrôlée des informations sensibles à l'extérieur. Une donnée interne à l'établissement ne doit pas être stockée à l'extérieur sans s'assurer que le contrat avec l'hébergeur garantie la protection des données conformément à la loi informatique de liberté, à la PSSI de l'état et la PSSI de l'UCBL.

2.5 Règles de sécurité liées au contexte de télétravail

En complément des règles applicables à l'ensemble des utilisateur·trices, les agents autorisés à exercer des fonctions en télétravail dans le cadre de la « Charte Télétravail des personnels BIATSS » doivent être particulièrement attentifs aux dispositions suivantes :

- le poste informatique utilisé dans le cadre du télétravail n'est en aucun cas un ordinateur familial ; aucun membre de la famille ou tiers ne doit être autorisé à y accéder ;
- le télétravailleur doit s'abstenir de consulter des documents, dès lors qu'ils ne sont pas publics, en présence d'une tierce personne ;
- les mots de passe permettant de déverrouiller le poste de travail, ou les comptes professionnels, ne doivent pas être confiés à des proches ou des tiers ;
- l'utilisation d'un filtre de confidentialité est recommandée.

Article 3 Protection des données à caractère personnel

3.1 Rappels sur la loi informatique et libertés

La loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

L'UCBL a désigné un·e correspondant·e à la protection des données à caractère personnel. Il·elle a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978. Il·elle est obligatoirement consulté·e par le responsable des traitements préalablement à leur création. Il·elle recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de l'université au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

Le·la correspondant·e veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir le·la correspondant·e (cil@univ-lyon1.fr).

3.2 Accès de l'employeur aux données stockées sur l'environnement informatique des personnels

Pour les personnels de l'université, les données (courriel et/ou fichier) dont le caractère privé n'est pas expressément mentionné sont réputées à caractère professionnel. L'employeur peut y avoir accès, pour les besoins du service, même sans l'accord des personnes concernées.

Notamment en cas d'absence ou de départ d'un personnel de l'université et afin de ne pas interrompre le fonctionnement du service, le·la RSSI peut ponctuellement transmettre au supérieur hiérarchique un courriel ou fichier sauf si l'agent l'a expressément identifié comme « privé ».
Seront considérés comme privés les données ou messages mentionnant expressément le caractère « privé » soit dans le titre ou le sujet, soit dans le fait de les regrouper dans un dossier nommé « privé ».
Les données ou messages identifiés comme « privés » ne peuvent être ouverts par l'employeur, sauf risque ou événement particulier, qu'en présence de l'agent ou celui-ci dûment appelé.

Article 4 Interventions du RSSI et des administrateurs

4.1 Définition du RSSI et des administrateurs

Le·la RSSI est désigné·e comme administrateur·trice du SI. Les administrateur·trices veillent à la protection, à la maintenance, à l'évolution, au bon fonctionnement du SI et veille au respect de la présente Charte par l'ensemble des utilisateur·trices.
Le·la RSSI est l'expert qui garantit la sécurité, la disponibilité et l'intégrité du système d'information et des données. Il·elle définit la politique de sécurité du SI et veille à son application.
Le·la RSSI et les administrateur·trices du SI ont accès à l'ensemble des données techniques pour assurer leurs missions mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents. Ils·elles sont assujetti·es au devoir de réserve et sont tenu·es de préserver la confidentialité des données qu'ils·elles sont amené·es à connaître dans le cadre de leurs fonctions.
En cas d'urgence, ils·elles peuvent prendre toute mesure conservatoire nécessaire à la protection du SI.

4.2 Disponibilité du service

L'université s'efforce, dans la mesure du possible de maintenir accessible le service qu'elle propose de manière permanente mais n'est tenue à aucune obligation d'y parvenir. L'université peut interrompre l'accès, notamment pour des raisons de maintenance, de mise à niveau et de sécurité sans pouvoir être tenue pour responsable des conséquences de ces interruptions tant à l'égard des utilisateur·trices que des tiers.

4.3 Contrôle et maintenance des administrateurs et RSSI

L'utilisateur·trice est averti·e que les administrateur·trices et le·la RSSI peuvent avoir accès à l'ensemble des composants du SI, et ce afin d'assurer la sécurité du SI et de garantir :

- La confidentialité, l'intégrité et la disponibilité des données.
- La preuve de la date de création ou de diffusion d'informations (traçabilité).
- La recherche et le rejet d'intrusions dans le SI ou de matériels violant les règles relatives au droit d'auteur.
- La mise à jour, maintenance, correction et réparation du SI.

Les administrateur·trices et le·la RSSI pourront mettre en place des outils de contrôle et de surveillance répondant strictement à la finalité de la protection du SI.
Tout utilisateur·trice peut obtenir auprès des administrateur·trices et du·de la RSSI les informations sur les moyens de contrôle mis en œuvre.
Les services techniques sont dans l'obligation d'effectuer des sauvegardes des données stockées sur les serveurs de l'université, y compris sur les contenus personnels, dans le but exclusif d'empêcher des pertes d'informations. Ces contenus bénéficient des mêmes protections en termes de confidentialité que les données d'origine.

4.4 Filtrages

L'université dispose de pare-feu pour protéger son réseau et limiter certains trafics. Le Centre inter-établissement pour les services réseaux (CISR) détermine les règles de filtrage : tout utilisateur·trice peut prendre connaissance de ces règles et faire une demande écrite et justifiée de modification de celles-ci.

4.5 Les logs

Le SI doit comprendre des mécanismes de journalisation protégés contre le sabotage et les accès non autorisés au SI. La durée de conservation des journaux informatiques est d'un an maximum, conformément à la loi. L'objectif est de permettre de :

- Contrôler l'utilisation de la ressource, détecter les anomalies afin de mettre en place une qualité de service et faire évoluer les équipements en fonction des besoins.
- Conserver une trace des actions réalisées par les administrateur·trices sur les systèmes et les applications pour permettre un retour en arrière ou une correction en cas de dysfonctionnement suite à une intervention d'un administrateur.
- Détecter des intrusions ou des utilisations frauduleuses, de tenter d'identifier les causes et les origines et de remettre en place le système.
- De fournir les éléments de preuves nécessaires pour mener les enquêtes en cas d'incident et de répondre à toute réquisition judiciaire.

Les RSSI ont accès à la totalité des journaux. Les administrateur·trices du SI ont accès uniquement aux logs de moins de trois mois des services qu'ils gèrent.

Article 5 Sanctions

Tout manquement aux règles de la présente Charte engage la responsabilité de l'utilisateur·trice. Le·la Président·e de l'université peut prendre toute mesure conservatoire à l'encontre de l'utilisateur·trice (suspension des droits d'accès, suppression d'un contenu etc.) sans préjudice d'éventuelles poursuites disciplinaires et/ou pénales.

Article 6 Entrée en vigueur

La présente charte sera affichée dès son adoption par le Conseil d'Administration et sera accessible sur l'Internet et l'Intranet de l'université. Elle est annexée au règlement intérieur. Elle annule et remplace la Charte approuvée par le Conseil d'Administration du 26 novembre 2002.