Charte informatique

Version 2021.1

1 Préambule

L'entreprise met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique, ainsi que des outils mobiles. Les salariés et collaborateurs, dans l'exercice de leurs fonctions, sont conduits à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'entreprise. L'utilisation du système d'information et de communication doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des salariés, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'entreprise. Elle ne remplace en aucun cas les lois en vigueur que chacun est censé connaître.

2 Champ d'application

2.1 Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, avocats collaborateurs, associés, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels. Elle sera annexée aux contrats de prestations. Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

2.2 Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques y compris clés USB, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, smartphones, tablettes et clés 3G, logiciels, fichiers, données et bases de données, système de messagerie, connexion internet, intranet, extranet, abonnements à des services interactifs. Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le

matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

2.3 Autres accords sur l'utilisation du système d'information

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élections par voie électronique ou la mise en télétravail de salariés.

3 Confidentialité

3.1 Paramètres d'accès

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 (identifiant, mot de passe). Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Ils ne doivent être communiqués à personne, ni responsable hiérarchique, ni informatique. 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. Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité et être modifiés régulièrement. Des consignes de sécurité sont élaborées par la direction ou la direction informatique afin de recommander les bonnes pratiques en la matière. Aucun utilisateur ne doit se servir pour accéder au système d'information de l'entreprise d'un autre compte que celui qui lui a été attribué. Il ne doit pas non plus déléguer à un tiers les droits d'utilisation qui lui sont attribués.

3.2 Données

Chaque utilisateur est responsable pour ce qui le concerne du respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication sont définies par la direction et applicables quel que soit le support de communication utilisé. L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à l'entreprise, dans des lieux autres que ceux de l'entreprise (hôtels, lieux publics…).

4 Sécurité

4.1 Rôle de l'entreprise

L'entreprise met en œuvre les moyens humains et techniques appropriés pour assurer la sécurité matérielle et logicielle du système d'information et de communication. À ce titre, il lui appartient de limiter les accès aux ressources sensibles et d'acquérir les droits de propriété intellectuelle ou d'obtenir les autorisations nécessaires à l'utilisation des ressources mises à disposition des utilisateurs. La direction informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et

de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

4.2 Responsabilité de l'utilisateur

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler à la direction informatique toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie. Sauf autorisation expresse de la direction, l'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (smartphone, supports amovibles…) est interdit. Dans le cas où il a été autorisé, il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité. De même, la sortie de matériel appartenant à l'entreprise doit être justifiée par des obligations professionnelles et nécessite l'accord exprès de la direction. 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. L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition en suivant les procédures définies par la direction informatique. Il doit régulièrement supprimer les données devenues inutiles sur les espaces communs du réseau ; les données anciennes mais qu'il souhaite conserver doivent être archivées avec l'aide de la direction informatique. L'utilisateur doit éviter d'installer ou de supprimer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il ne doit pas non plus modifier les paramétrages de son poste de travail ou des différents outils mis à sa disposition, ni contourner aucun des systèmes de sécurité mis en œuvre dans l'entreprise. Il doit dans tous les cas en alerter la direction informatique. L'utilisateur s'oblige en toutes circonstances à se conformer à la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

5 Internet

5.1 Accès aux sites

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites. Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'Internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est aussi prohibé de créer ou mettre à jour au moyen de l'infrastructure de l'entreprise tout site Internet, notamment des pages personnelles. Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à

ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci.

5.2 Autres utilisations

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, chats, blogs n'est autorisée qu'à titre professionnel et sur autorisation expresse de la hiérarchie qui devra en informer la direction informatique. De même, tout téléchargement de fichier, en particulier de fichier média, est prohibé, sauf justification professionnelle dûment validée par la hiérarchie. Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'entreprise. Ils sont informés que la direction informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'entreprise.

6 Messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique normalisée attribuée par la direction informatique. Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer la direction informatique des dysfonctionnements qu'ils constateraient dans ce dispositif de filtrage.

6.1 Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier postal : il obéit donc aux mêmes règles, en particulier en matière d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à son supérieur. Un message électronique peut être communiqué très rapidement à des tiers et il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et de l'utilisateur. Avant tout envoi, il est impératif de bien vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'informations à caractère confidentiel, ces vérifications doivent être renforcée. En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires. En cas d'envoi à une liste de diffusion, il est important d'en vérifier les modalités d'abonnement, de contrôler la liste des abonnés et de prévoir l'accessibilité aux archives. 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 doivent être envoyés avec un accusé de réception ou signés électroniquement. Ils doivent, le cas échéant, être doublés par un envoi de courrier postal. Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent pas comporter d'éléments illicites, tels

que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire. La forme des messages professionnels doit respecter les règles définies par la direction, pour ce qui concerne la mise en forme et surtout la signature des messages. En cas d'absence supérieure à 3 jours, le salarié doit mettre en place un répondeur automatique.

6.2 Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par la direction informatique. Cette limite est susceptible d'être levée temporairement ou définitivement sur demande adressée à la direction informatique, qui est aussi chargée de l'ouverture des listes de diffusion qui pourraient s'avérer nécessaires. De même, la direction informatique peut limiter la taille, le nombre et le type des pièces jointes pour éviter l'engorgement du système de messagerie. Pour des raisons de capacité mémoire, les messages électroniques sont conservés sur le serveur de messagerie jusqu'à saturation. Passé ce volume, la messagerie sera bloquée. Si le salarié nécessite une extension du volume de stockage de sa messagerie, il formulera une demande à la direction informatique. Il est aussi tenu de supprimer lui-même dès que possible tous les messages inutiles.

6.3 Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte. Les messages envoyés doivent être signalés par la mention "Privé" ou "Perso" dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé de la même façon. Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel. Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

6.4 Utilisation de la messagerie par la délégation du personnel

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel, mais en utilisant la mention "Délégué" dans leur objet à l'émission et dans le dossier où ils doivent être classés.

7 Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ou clé 3G. Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière. De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles rappelées plus haut. Enfin, les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie en cas d'urgence professionnelle.

7.1 Utilisation personnelle de la téléphonie

L'utilisation à caractère personnel du téléphone, fixe ou mobile, est tolérée, à condition qu'elle reste dans des limites raisonnables en termes tant de temps passé que de quantité d'appels. Les surcoûts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles devront être remboursés par les utilisateurs concernés. Il s'agit tout particulièrement des appels à des numéros surtaxés et des appels depuis l'étranger ou à destination de l'étranger, au sens de la facturation téléphonique. Les utilisateurs sont informés que la direction informatique enregistre leur activité téléphonique, aussi bien sur les postes fixes que sur les mobiles. Ces traces seront exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi. Toutefois, seule la direction pourra avoir accès aux numéros détaillés, permettant d'identifier les interlocuteurs d'un utilisateur, et seulement en cas de différend avec lui.

8 Respect de la loi informatique et libertés et du RGPD

Pour tout traitement de données personnelles, l'utilisateur se conformera au règlement (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, le RGPD. L'utilisateur est informé que les données à caractère personnel le concernant sont conservées par le service informatique pendant toute la durée de leur relation contractuelle et des délais en matière de prescription. L'utilisateur est informé qu'il dispose, pour des motifs légitimes admis par l'entité, des droits conformes au RGPD tels que droit d'accès, de rectification, d'opposition, droit à l'effacement, à la portabilité, à la limitation du traitement, relatifs à l'ensemble des informations le concernant. Le CAES du CNRS a désigné un Délégué à la Protection des Données personnelles, le DPO ou DPD, et un DPO référant pour le CNRS. Le DPO ou DPD a pour mission d'informer, de conseiller et de veiller à la conformité des traitements à la réglementation en matière de données personnelles. Il doit être consulté préalablement à la création d'un traitement (mise en place d'un fichier de données personnelles). Il veille au respect des droits des personnes et peut être sollicité via l'adresse mail suivante : donneespersonnelles@onelaw.fr

9 Contrôle des activités

9.1 Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux ("logs"), créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information. Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication.

Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers ;

- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites ou le téléchargement de fichiers ;
- Aux appels téléphoniques émis ou reçus à partir des postes fixes ou mobiles pour surveiller le volume d'activités et détecter des dysfonctionnements. L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges.

Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur. Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la direction. De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

9.2 Procédure de contrôle manuel

En cas de dysfonctionnement constaté par la direction informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs. Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à sa disposition ou sur le réseau de l'entreprise, ou sur sa messagerie. Alors, sauf risque ou événement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte, qu'en présence de l'utilisateur ou celui-ci dûment appelé et éventuellement représenté par un délégué du personnel.

10 Respect de la propriété intellectuelle

L'utilisateur ne doit pas reproduire, télécharger, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation des titulaires de ces droits.

11 Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié par voie électronique. La direction informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde et de filtrage. Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur sa sécurité. Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte. En cas de besoin, les salariés pourront être formés par la direction informatique pour appliquer les règles d'utilisation du système d'information et de communication prévues. Le manquement aux règles et mesures de sécurité décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions

disciplinaires, proportionnées à la gravité des faits concernés. Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées. L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de l'entreprise donnera également lieu à remboursement de la part de l'utilisateur concerné. Le Représentant de l'entreprise ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret des correspondances.

12 Rappel des principales dispositions légales

Il est rappelé que l'ensemble des agents CNRS quel que soit leur statut sont soumis à la législation française en vigueur et notamment :

► la loi du 29 juillet 1881 modifiée sur la liberté de la presse,

► la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés,

► la législation relative aux atteintes aux systèmes de traitement automatisé de données (art. L 323-1 et suivants du code pénal),

► la loi n° 94-665 du 4 août 1994 modifiée relative à l'emploi de la langue française, 2 Il s'agit des données classifiées de défense qui couvre le « confidentiel défense », le « secret défense » et le « très secret défense ». CAES DU CNRS CHARTE INFORMATIQUE Mars 2021 Page : 5 / 5 CAES DU CNRS - Charte Informatique - 2021

► la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique,

► le règlement européen pour la protection des données personnelles (UE) n°2016/679 promulgué par la loi d'application n°2018-493 du 20 juin 2018

► les dispositions du code de propriété intellectuelle relative à la propriété littéraire et artistique

13 Entrée en vigueur

La présente charte est applicable à compter du 1er janvier 2021

Elle a été adoptée après information et consultation des salariés et collaborateurs

Fait à LYON le 15 décembre 2020

L'employeur (signature) : Maître Gabriel Rigal, associé gérant