lojelis
TECH AND HUMAN INNOVATION

ANNEXE AU RÈGLEMENT INTÉRIEUR :

CHARTE INFORMATIQUE

Lojelis 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, 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 être effectuée 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, la présente charte pose les règles relatives à l'utilisation de ces ressources.

Elle définit également 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 dans le cadre de la responsabilité civile et pénale 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 connaitre.

Article 1 – Champ d'application

1.1. 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 dirigeants, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels.

Les salariés veillent à faire accepter les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

1.2. 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, télévisions, réseau informatique (serveurs, routeurs et connectique), imprimantes, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet.

La composition du système d'information et de communication est indifférente à la propriété sur les éléments qui le composent.

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.

Article 2 – Documents de référence

Numéro	Nom du document	Référence / Version	Date	Origine
1	Modèle de charte rédigé par David Melison, membre du Centre d'étude et de recherches en droit de l'immatériel (Cerdi)	Extrait de « Formulaire commenté Lamy Droit de l'immatériel », aux Editions Lamy	17/04/2007	Editions Lamy
2	Note technique Recommandations de sécurité relatives aux mots de passe	NP_MDP_NoteTech.pdf V1.1	05/06/2012	ANSSI

Article 3 – Confidentialité

1.1. 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, certaines applications ou services interactifs) est protégé par des paramètres de connexion (identifiants, mots de passe).

Ces paramètres sont personnels à l'utilisateur et doivent être gardés confidentiels. Ils permettent en particulier de contrôler l'activité des utilisateurs. Toutefois, pour des raisons de sécurité et de persistance des données, ils peuvent être communiqués à la Direction.

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 l'ANSSI afin de recommander les bonnes pratiques en la matière (voir la Note technique Recommandations de sécurité relatives aux mots de passe).

Sauf demande formelle de la Direction, 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.

Si un employé est absent, Lojelis peut lui demander de communiquer son mot de passe lorsque les informations détenues par cet employé sont nécessaires à la poursuite de l'activité de l'entreprise.

1.2. 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 applicable 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, …).

Article 4 – Sécurité et protection des données

1.1. Rôle de l'entreprise

Lojelis 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.

Le service infrastructure est en charge du contrôle du bon fonctionnement du système d'information et de communication. Il veille à l'application des règles de la présente charte. Il est assujetti à une obligation de confidentialité sur les informations qu'il est amené à connaître.

1.2. 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.

L'Utilisateur s'engage à prendre soin et à conserver en bon état le matériel informatique (ordinateur portable, écran, souris, casque, …) qui lui est confié dans le cadre de l'exécution de son travail. Il est recommandé de ne pas boire ou manger à proximité des PCs.

En particulier, il doit signaler au service infrastructure toute violation ou tentative de violation de l'intégrité de ces ressources et, de manière générale tout dysfonctionnement, incident ou anomalie.

Le fait de détériorer volontairement le matériel peut être considérer comme une faute grave ou lourde.

L'utilisateur s'engage à respecter les règles énoncées ci-dessous dans le but de veiller au bon fonctionnement des ressources informatiques mis à sa disposition.

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.

En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (smartphone, supports amovibles), il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

L'utilisateur doit utiliser le répertoire « OneDrive - Lojelis » afin d'assurer la sauvegarde de ses données professionnelles.

Le répertoire « OneDrive - Lojelis » est un espace de stockage nominatif. Son contenu n'est pas accessible aux autres utilisateurs et, étant hébergé sur le cloud Microsoft lié à Office365, il est disponible de n'importe où depuis Internet

L'utilisateur doit éviter d'installer 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 le service infrastructure Lojelis.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de 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.

Article 5 – Accès à internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le service infrastructure. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

La contribution des utilisateurs avec la création de compte Lojelis à des forums de discussion, systèmes de discussion instantanée, blogs, sites est autorisée, en transmettant les informations de connexion niveau service infrastructure. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Des comptes nominatifs utilisant l'adresse email Lojelis peuvent être créé à condition de vérifier préalablement l'existence auprès du service infrastructure d'un compte impersonnel Lojelis utilisable ou d'un groupe auquel se rattacher.

Exemples : Webex

- Un compte Lojelis existe sans limitations (nombre de participants, …) : demander les accès au service infrastructure.
- Un compte nominatif gratuit peut être créé (voir les limitations sur le site https://www.webex.com/)

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

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.

Les sites Internet consultés via les PC Lojelis font l'objet d'un contrôle antiviral et d'un filtrage par catégories de contenu. Les salariés sont invités à informer la Direction des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

Article 6 – Utilisation des imprimantes

Pour raisons économiques et environnementales, évitez autant que possible d'imprimer.

Synthèse des bonnes pratiques pour imprimer :

- Enregistrement au format PDF à l'aide d'une imprimante virtuelle (par exemple *PDF creator*).
- Imprimer en recto-verso.
- Utiliser la fonction réduction.
- Imprimer de préférence en noir et blanc plutôt qu'en couleur.
- Eviter d'imprimer des documents comportant de grandes surfaces sombres, peu lisibles et très consommatrices d'encre.
- Si l'imprimante dispose de cette fonction, imprimer les documents en mode économie.

Article 7 – Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le service infrastructure. La messagerie est accessible aussi bien à partir d'un logiciel de messagerie qu'à partir d'un navigateur Internet grâce à un Webmail.

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 des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

1.1. 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 termes 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/ou de l'utilisateur.

Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises. En présence d'information à caractère confidentiel, ces vérifications doivent être renforcées.

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.

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 comporter aucun élément illicite, tel 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 dans la charte graphique de Lojelis, notamment en ce qui concerne la mise en forme et la signature des messages.

Si besoin, lors d'une absence prolongée, un répondeur automatique d'email peut être mis en place dans les paramètres de la messagerie ou sur demande auprès du service infrastructure.

1.2. Limites techniques

Pour des raisons techniques, l'envoi de messages électroniques n'est possible, directement, que vers un nombre limité de destinataires, fixé par notre prestataire de messagerie.

De même, la taille, le nombre et le type des pièces jointes peuvent être limités par notre prestataire de messagerie.

1.3. Listes de diffusion

Afin de faciliter la communication et l'envoi de mails en masse en interne, plusieurs listes de diffusion sont ouvertes par le service infrastructure :

- collaborateurs@lojelis.com : pour envoyer un mail à l'ensemble des collaborateurs de Lojelis.
- agence-clermont@lojelis.com : pour envoyer un mail uniquement aux collaborateurs rattachés à l'agence clermontoise.
- agence-paris@lojelis.com : pour envoyer un mail uniquement aux collaborateurs rattachés à l'agence parisienne.
- agence-lyon@lojelis.com : pour envoyer un mail uniquement aux collaborateurs rattachés à l'agence lyonnaise.
- agence-lille@lojelis.com : pour envoyer un mail uniquement aux collaborateurs rattachés à l'agence lilloise.

L'utilisation des mail-listings est soumise à modération pour éviter tout abus. Les messages électroniques passant par une liste de diffusion devront donc être validés par les modérateurs avant leur diffusion.

1.4. 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 " [Personnel] " ou " [Perso] " dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé "Privé" ou "Personnel" ou "Perso". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé "Privé" ou "Personnel" ou "Perso". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de message à caractère personnel.

Utilisation de la messagerie pour la communication destinée aux institutions représentatives 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 "CSE" dans leur objet à l'émission et dans le dossier où ils doivent être classés.

1.5. Fermeture du compte de messagerie

Le service infrastructure avertit le salarié de la date de fermeture de son compte de messagerie afin que ce dernier puisse vider son espace privé. Par défaut la fermeture de compte intervient cinq jours ouvrés après le départ.

Article 8 – Données personnelles

Conformément au Règlement Général sur la Protection des Données (RGPD), Lojelis tient à la disposition des salariés *un registre des traitements de données* regroupant l'ensemble des traitements et des informations personnelles récoltées. Ce registre permet aux autorités et aux salariés, en vertu de leur droit d'accès, de savoir quelles sont les données recueillies, et les finalités de leur traitement.

Ce registre ainsi que le détail des activités de traitement de données personnelles sont disponibles sur le SharePoint à l'adresse suivante :

https://lojelis.sharepoint.com/SitePages/RGPD.aspx

Conformément au RGPD du 25 mai 2018, vous disposez d'un droit d'accès, de portabilité, de rectification, de limitation, de consentement, d'actualisation et de suppression de vos données personnelles.

Vous pouvez exercer ces droits en adressant un email à la personne en charge de la protection des données à l'adresse email suivante : dpo@lojelis.com.

Article 9 – Contrôle des activités

1.1. 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 suppression 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 web ou le téléchargement de fichiers.

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.

1.2. Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service infrastructure, il peut procéder 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.

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 représentant du personnel.

1.3. Pare-feu

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique, l'échange de fichiers et la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- de la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels);
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe (et éventuellement texte du message).

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionniste ou contenant des données jugées comme offensantes.

Article 10 – Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier sur un emplacement compris dans le plan de sauvegarde n'est pas absolue et qu'il en reste une copie :

- Sur le serveur ;
- Sur le dispositif de sauvegarde miroir ;

Article 11 – Sanctions

Le manquement aux règles et mesures de sécurité de 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 la gravité des faits concernés.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

Article 12 – Information des salariés

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.

Le service infrastructure est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC. Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur le SharePoint de l'entreprise.

Des opérations de communication internes seront organisées ponctuellement afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

Article 13 – Entrée en vigueur

La présente charte est applicable à compter du 9 Mars 2020.