Charte de l'utilisateur du système d'information d'Elior group

Version 2015

Préambule

Le "**système d'information**" recouvre l'ensemble des ressources matérielles, logicielles, applications, bases de données et réseaux de télécommunications, pouvant être mis à disposition par l'entreprise. L'informatique nomade (les ordinateurs portables, les téléphones portables, les ordiphones...) est également un des éléments constitutifs du système d'information.
Pour des raisons de sécurité de l'information, est également considéré comme faisant partie du système d'information, le matériel personnel des salariés connecté au réseau de l'entreprise ou contenant des informations à caractère professionnel concernant l'entreprise.
Par **"entreprise"** il faut entendre toute société ou entité juridique du groupe Elior.
Le terme d'**"utilisateur"** recouvre tout personnel ayant accès, dans le cadre de l'exercice de son activité professionnelle, aux ressources du système d'information quel que soit son statut.
Il s'agit notamment de :

- tout collaborateur (salariés, stagiaires, mandataires sociaux, ...)
- tout prestataire[1] ayant contracté avec l'entreprise.

Le bon fonctionnement du système d'information suppose le respect des dispositions législatives et réglementaires, notamment le respect des règles visant à assurer la sécurité, la performance des traitements et la conservation des données.
La présente charte définit les règles d'usages et de sécurité que l'entreprise et l'utilisateur s'engagent à respecter : elle précise les droits et devoirs de chacun.

La charte peut être complétée par des guides d'utilisation définissant les principales règles et pratiques d'usage.

Cette charte a pour vocation de **prendre en compte des recommandations des autorités compétentes** (telles que la CNIL, l'Hadopi ou l'ANSSI) et de **se mettre en conformité aux nouveaux usages des systèmes d'information.**

Engagements de l'entreprise :

- L'entreprise porte à la connaissance de l'utilisateur la présente charte.
- L'entreprise met en œuvre les mesures nécessaires pour assurer la sécurité du système d'information et la protection des données des utilisateurs.
- L'entreprise facilite l'accès des utilisateurs aux ressources du système d'information. Les ressources mises à leur disposition sont prioritairement à usage professionnel mais l'entreprise est tenue de respecter l'utilisation résiduelle du système d'information à titre privé.

Engagements de l'utilisateur :

- L'utilisateur est responsable, en tout lieu, de l'usage qu'il fait du système d'information auquel il a accès.
- Il a une obligation de réserve et de confidentialité à l'égard des informations et documents auxquels il accède. Cette obligation implique le respect des règles d'éthique professionnelle et de déontologie.
- En tout état de cause, l'utilisateur est soumis au respect des obligations résultant de son statut ou de son contrat.

[1] Le contrat devra prévoir expressément l'obligation de respect de la charte

Article I. Champ d'application

Les règles d'usage et de sécurité figurant dans la présente charte s'appliquent à l'entreprise ainsi qu'à l'ensemble des utilisateurs.
La présente Charte est sans préjudice des accords particuliers pouvant porter, le cas échéant, sur l'utilisation du système d'information et de communication de l'entreprise par les institutions représentatives, l'organisation d'élections par voie électronique ou le télétravail.

Article II. Conditions d'utilisation des systèmes d'information

2.01 Utilisation professionnelle / privée

Les systèmes d'information (notamment messageries, internet ...) sont des outils de travail ouverts à des usages professionnels.
Ils peuvent également constituer le support d'une communication privée dans les conditions décrites ci-dessous.

L'utilisation résiduelle du *système d'information* à titre privé doit être non lucrative et raisonnable, tant dans sa fréquence que dans sa durée. En toute hypothèse, le surcoût qui en résulte doit demeurer négligeable au regard du coût global d'exploitation.
Cette utilisation ne doit pas nuire à la qualité du travail de l'utilisateur, au temps qu'il y consacre et au bon fonctionnement du service.
Toute information est réputée professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée.
Ainsi, il appartient à l'utilisateur de procéder au stockage de ses données à caractère privé dans un espace de données prévu à cet effet ou en mentionnant explicitement[2] le caractère privé. La sauvegarde régulière des données à caractère privé incombera à l'utilisateur.
L'utilisateur est responsable de son espace de données à caractère privé. Lors de son départ définitif du service ou de l'entreprise, il lui appartient de détruire son espace de données à caractère privé, la responsabilité de l'entreprise ne pouvant être engagée quant à la conservation de cet espace. Les mesures de conservation des données professionnelles sont définies avec le responsable désigné au sein de l'entreprise.

2.02 Continuité de service : gestion des absences et des départs

Aux seules fins d'assurer la continuité de service, l'utilisateur informe sa hiérarchie des modalités[3] permettant l'accès aux ressources mises spécifiquement à sa disposition.
En cas d'absence non planifiée de l'utilisateur et pour des raisons exceptionnelles, si l'administrateur se trouve dans l'obligation de modifier les codes d'accès au système d'information de l'utilisateur, il doit en informer ce dernier qui procédera à leur changement dès que possible.

2.03 Utilisations interdites

L'utilisation des systèmes d'information doit respecter la réglementation en vigueur.
En particulier, la détention, diffusion et exportation d'images à caractère pédophile[4], ou la diffusion de contenus à caractère raciste ou antisémite[5] est totalement interdite.
Par ailleurs, la consultation de sites de contenus à caractère pornographique depuis le système d'information de l'entreprise est interdite.

[2] Par exemple, cet espace pourrait être dénommé "_privé_"
[3] à titre exemple, en cas d'absence ou de départ, si nécessaire, il pourra communiquer à sa hiérarchie les mots de passe d'accès au système d'information

[4] Article L 323-1 et s. du Code pénal

[5] Article 24 et 26bis de la Loi du 29 juillet 1881

Article III. Principes de sécurité

Section 3.01 Règles de sécurité applicables

L'entreprise met en œuvre les mécanismes de protection appropriés sur les systèmes d'information mis à la disposition des utilisateurs.
L'utilisateur est informé que les codes d'accès constituent une mesure de sécurité destinée à éviter toute utilisation malveillante ou abusive. Cette mesure ne confère pas aux outils informatiques protégés un caractère personnel.

Les niveaux d'accès ouverts à l'utilisateur sont définis en fonction de la mission qui lui est confiée.
La sécurité des systèmes d'information mis à sa disposition lui impose :

- de respecter les consignes de sécurité, notamment les règles relatives à la gestion des codes d'accès ;
- de garder strictement confidentiels son (ou ses) codes d'accès et ne pas le(s) dévoiler à un tiers; (sauf cas prévu en section 2.02)
- de respecter la gestion des accès, en particulier ne pas utiliser les codes d'accès d'un autre utilisateur, ni chercher à les connaître ;
- en cas d'absence, même temporaire, de verrouiller l'accès au système d'information qui lui est propre.

Par ailleurs, la sécurité des ressources mises à la disposition de l'utilisateur nécessite plusieurs précautions de la part de l'entreprise :

- veiller à ce que les ressources sensibles ne soient accessibles qu'aux personnes habilitées, en dehors des mesures d'organisation de la continuité du service mises en place par la hiérarchie. (Sauf cas prévu en section 2.02)
- limiter l'accès aux seules ressources pour lesquelles l'utilisateur est expressément habilité ;

De la part de l'utilisateur :

- s'interdire d'accéder ou de tenter d'accéder à des ressources du système d'information, pour lesquelles il n'a pas reçu d'habilitation explicite ;
- ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés par l'entreprise ;
- ne pas installer, télécharger ou utiliser sur le matériel de l'entreprise, des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, ou sans autorisation de la Direction des Systèmes d'Information ;
- se conformer aux dispositifs mis en place par l'entreprise pour lutter contre les virus et les attaques par programmes informatiques ;
- ne pas utiliser sans accord explicite de la Direction des Systèmes d'Information de logiciel ou d'application personnels pour des usages professionnels ;

Section 3.02 Devoirs de signalement et d'information

L'utilisateur doit avertir la Direction des Systèmes d'Information dans les meilleurs délais de tout dysfonctionnement constaté ou de toute anomalie découverte telle une intrusion dans le système d'information, etc. Il doit également signaler à son responsable hiérarchique toute possibilité d'accès à une ressource qui ne correspond pas à son habilitation.

Section 3.03 Mesures de contrôle de la sécurité

L'utilisateur est informé :

- que pour effectuer la maintenance corrective, curative ou évolutive, l'entreprise se réserve la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition ;
- qu'une maintenance à distance ne peut s'effectuer sans l'avoir préalablement informé ;
- que toute information bloquante pour le système ou générant une difficulté technique d'acheminement à son destinataire, sera isolée et le cas échéant, supprimée.

L'entreprise informe l'utilisateur que le système d'information donne lieu à une surveillance et un contrôle à des fins statistiques, de traçabilité réglementaire ou fonctionnelle, d'optimisation, de sécurité ou de détection des abus, dans le respect de la législation applicable.
L'entreprise est dans l'obligation légale de mettre en place un système de journalisation[6] et de filtrage[7] des accès Internet, de la messagerie et des données échangées.
Préalablement à cette mise en place, l'entreprise procèdera, auprès de la Commission Nationale de l'Informatique et des Libertés, à une déclaration, qui mentionnera notamment la durée de conservation des traces et durées de connexions, les conditions du droit d'accès dont disposent les utilisateurs, en application de la loi n° 78-17 du 6 janvier 1978 modifiée.

Les personnels chargés des opérations de contrôle des systèmes d'information sont soumis au secret professionnel. Ils ne peuvent divulguer les informations qu'ils sont amenés à connaître dans le cadre de leurs fonctions dès lors que ces informations sont couvertes par le secret des correspondances ou identifiées comme telles.
En revanche, ils doivent communiquer ces informations si elles mettent en cause le bon fonctionnement technique des applications ou leur sécurité.

Section 3.04 Utilisation de matériel privé sur l'infrastructure de l'entreprise

Les utilisateurs amenés à utiliser leur équipement non fourni par l'entreprise dans un but professionnel doivent bénéficier de l'accord de leur hiérarchie et de la Direction des Systèmes d'Information qui s'assurera du bon niveau de sécurité de leur équipement (ex : antivirus, mise à jour du système ...) afin de ne pas perturber le fonctionnement du système d'information. L'entreprise pourra imposer l'installation d'un logiciel de contrôle afin de s'assurer du respect des prérequis spécifiés.

Dans le cas où un équipement privé ne respecterait pas les prérequis techniques et bonnes pratiques de sécurité, la Direction des Systèmes d'Information, se réserve le droit :

- d'interrompre sans délais son accès au système d'information ;
- de supprimer les informations professionnelles stockées sur cet équipement.

[6] Conservation des informations techniques de connexion telles que l'heure d'accès, l'adresse IP de l'utilisateur

[7] La mise en œuvre du filtrage d'accès aux sites web nécessite, quand cela est nécessaire (sites https), de déchiffrer les données échangées entre le poste utilisateur et le site web. Cette analyse n'est pas réalisée au cas par cas, mais de manière globale ; les données déchiffrées ne sont pas enregistrées (informations inaccessibles). La journalisation des flux déchiffrés est équivalente à celle configurée pour les flux HTTP standards (heure, compte utilisateur, URL du site internet accédé, autorisation d'accès, virus identifié) ; aucune autre information n'est enregistrée

Article IV Communications électroniques

Section 4.01 Messagerie électronique

L'utilisation de la messagerie, la messagerie instantanée, les forums d'entreprise, ou réseaux sociaux d'entreprise, constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'échange de l'information au sein de l'entreprise.

(a) Adresses électroniques

L'entreprise pourra mettre à la disposition de l'utilisateur dont la fonction le nécessite, une boîte à lettres électronique professionnelle et nominative lui permettant d'émettre et de recevoir des messages.
L'aspect nominatif de l'adresse électronique constitue le simple prolongement de l'adresse administrative : il ne retire en rien le caractère professionnel de la messagerie.
L'adresse électronique nominative est attribuée à un utilisateur qui la gère sous sa responsabilité.
Une adresse électronique, fonctionnelle ou organisationnelle, peut être mise en place pour un utilisateur ou un groupe d'utilisateurs pour les besoins de l'entreprise.
La gestion d'adresses électroniques correspondant à des listes de diffusion, désignant une catégorie ou un groupe d'«utilisateurs», relève de la responsabilité exclusive de l'entreprise : ces listes ne peuvent être utilisées sans autorisation explicite.

(b) Contenu des messages électroniques

Tout message est réputé professionnel sauf s'il comporte une mention particulière et explicite indiquant son caractère privé[8] ou s'il est stocké dans un espace privé de données.
Pour préserver le bon fonctionnement des services, des limitations peuvent être mises en place : dans ce cas, les termes en sont précisés et portés à la connaissance de l'utilisateur par le fournisseur de service de messagerie.
Sont interdits les messages comportant des contenus à caractère illicite quelle qu'en soit la nature. Il s'agit notamment des contenus contraires aux dispositions de la loi sur la liberté d'expression ou portant atteinte à la vie privée d'autrui (par exemple : atteinte à la tranquillité par les menaces, atteinte à l'honneur par la diffamation, atteinte à l'honneur par l'injure non publique, protection du droit d'auteur, protection des marques...).

(c) Émission et réception des messages

L'utilisateur doit s'assurer de l'identité et de l'exactitude des adresses des destinataires des messages. Il doit veiller à ce que la diffusion des messages soit limitée aux seuls destinataires concernés afin d'éviter les diffusions de messages en masse, l'encombrement inutile de la messagerie ainsi qu'une dégradation du service. Par ailleurs, il s'interdit de paramétrer tout mécanisme de transfert automatique de messages reçus sur sa messagerie professionnelle vers une autre messagerie.

(d) Statut et valeur juridique des messages

Les messages électroniques échangés avec des tiers peuvent, au plan juridique, former un contrat, sous réserve du respect des conditions fixées par les articles[9] 1369-1 à 1369-11 du code civil.
L'utilisateur doit, en conséquence, être vigilant sur la nature des messages électroniques qu'il échange au même titre que pour les courriers traditionnels.

(e) Stockage et archivage des messages

L'entreprise n'est pas responsable de la conservation légale des éléments de preuve stockés dans la messagerie électronique. Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou simplement utiles en tant qu'éléments de preuve.

[8] Par exemple, les messages comportant les termes ("privé") dans l'objet ou sujet du message

[9] Issus de la loi n° 2004-575 du 21 juin 2004, ces articles fixent certaines obligations pour la conclusion des contrats en ligne

Section 4.02 Internet

Il est rappelé qu'Internet est soumis à l'ensemble des règles de droit en vigueur. L'utilisation d'Internet (par extension intranet) constitue l'un des éléments essentiels d'optimisation du travail, de mutualisation et d'accessibilité de l'information au sein et en dehors de l'entreprise.
Internet est un outil de travail ouvert à des usages professionnels. Si une utilisation résiduelle privée, telle que définie en section 2.01, peut être tolérée, il est rappelé que les connexions établies grâce à l'outil informatique mis à disposition par l'entreprise sont présumées avoir un caractère professionnel. L'entreprise peut les analyser à des fins d'amélioration du service.

(a) Publication sur les sites internet et intranet de l'entreprise

Toute publication de pages d'information sur les sites internet ou intranet de l'entreprise[10] doit être validée par un responsable de site ou responsable de publication nommément désigné.
Aucune publication de pages d'information à caractère privé (pages privées ...) sur les ressources du système d'information de l'entreprise n'est autorisée, sauf disposition particulière précisée dans un guide d'utilisation établi par le service ou l'entreprise.

(b) Sécurité

L'Entreprise se réserve le droit de filtrer ou d'interdire l'accès à certains sites, de procéder au contrôle a priori ou a posteriori des sites visités et des durées d'accès correspondantes.
Cet accès n'est autorisé qu'au travers des dispositifs de sécurité mis en place par l'entreprise.
L'utilisateur est informé des risques et limites inhérents à l'utilisation d'Internet par le biais d'actions de formations ou de campagnes de sensibilisation.

Section 4.03 Téléchargements

Tout téléchargement de fichiers, notamment de sons ou d'images, sur Internet doit s'effectuer dans le respect des droits de la propriété intellectuelle tels que définis à l'article V.
L'entreprise se réserve le droit de limiter le téléchargement de certains fichiers pouvant se révéler volumineux ou présenter un risque pour la sécurité des systèmes d'information (virus susceptibles d'altérer le bon fonctionnement du système d'information de l'entreprise, codes malveillants, programmes espions ...).

Article V. Respect de la propriété intellectuelle

L'entreprise rappelle que l'utilisation des ressources informatiques implique le respect de ses droits de propriété intellectuelle ainsi que ceux de ses partenaires et plus généralement, de tous tiers titulaires de tels droits.
En conséquence, chaque utilisateur doit :

- utiliser les logiciels dans les conditions des licences souscrites ;
- ne pas reproduire, copier, diffuser, modifier ou utiliser les logiciels, bases de données, pages web, textes, images, photographies ou autres créations protégées par le droit d'auteur ou un droit privatif, sans s'être assuré que l'entreprise a obtenu préalablement l'autorisation des titulaires de ces droits.

Article VI. Respect de la loi informatique et libertés

L'utilisateur est informé de la nécessité de respecter les dispositions légales en matière de traitement automatisé de données à caractère personnel, conformément à la loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés» modifiée, par la loi n° 2004-801 du 6 août 2004.
Les données à caractère personnel sont des informations qui permettent - sous quelque forme que ce soit - directement ou indirectement, l'identification des personnes physiques auxquelles elles s'appliquent.
Par ailleurs, conformément aux dispositions de cette loi, chaque utilisateur dispose d'un droit d'accès et de rectification relatif à l'ensemble des données le concernant, y compris les données portant sur l'utilisation des systèmes d'information.
Ce droit s'exerce auprès du responsable hiérarchique du service ou de l'entreprise dont il dépend.

[10] A partir des ressources informatiques mises à la disposition de l'utilisateur

Article VII. Limitation des usages

En cas de non-respect des règles définies dans la présente charte et des modalités définies dans les guides d'utilisation établis par le service ou l'entreprise, la «personne juridiquement responsable» pourra, sans préjuger des poursuites ou procédures de sanctions pouvant être engagées à l'encontre des personnels, limiter les usages par mesure conservatoire.
Tout abus dans l'utilisation des ressources mises à la disposition de l'utilisateur à des fins extraprofessionnelles est passible de sanctions.

Article VIII. Entrée en vigueur de la charte

Tout document relatif aux conditions d'utilisation du système d'information doit se conformer aux principes de cette charte.
La présente charte a valeur de règlement intérieur pour ce qui concerne l'usage des systèmes d'information.
Elle est annexée au règlement intérieur des sociétés du groupe Elior.
Elle fait également l'objet d'une communication devant le Comité de Direction des sociétés du groupe.
Le présent document prévaut sur tout autre document ou charte relatif à l'utilisation des systèmes d'information.

La présente Charte a fait l'objet d'une information consultation du Comité d'Entreprise ainsi que, pour les matières relevant de sa compétence, du Comité d'Hygiène, de sécurité et des conditions de travail. Elle a également été communiquée à l'Inspection du travail et déposée au secrétariat greffe du conseil de prud'hommes de Paris.

Elle entre en vigueur au sein de l'entreprise le 01 septembre 2016.

La présente charte est affichée dans les locaux de l'entreprise dans les mêmes conditions que le règlement intérieur. Elle fait par ailleurs l'objet d'une communication individuelle à chaque utilisateur du système d'information de l'entreprise.