

Charte des systèmes d'information

SOMMAIRE

1. PREAMBULE 4

2. PORTEE ET OPPOSABILITE 4

3. CHAMP D'APPLICATION 4
3.1. Personnes concernées 4
3.2. Moyens concernés 5
3.3. Usages concernés 5

4. CONDITIONS GENERALES D'UTILISATION 5
4.1. Usage professionnel 5
4.2. Usage non professionnel 6
4.3. Conditions d'accès et d'identification 8
4.3.1. Principes généraux relatifs à la gestion des droits d'accès 8
4.3.2. Modification / suspension des accès 9
4.4. Gestion des absences et des départs 9

5. CONDITIONS SPECIFIQUES D'UTILISATION 10
5.1. Mobilité et accès distant 10
5.2. Prêt de matériel informatique ou téléphonique 10
5.3. Télétravail 10
5.4. Materiel personnel utilisé à des fins professionnelles 10
5.5. Gestion des connaissances et de l'espace collaboratif 10
5.6. Médias sociaux 11
5.6.1. Usage professionnel 11
5.6.2. Usage non professionnel 11
5.6.3. Signalement 12

6. PROTECTION DE LA PROPRIETE INTELLECTUELLE, DES INFORMATIONS ET DES DONNEES 12
6.1. Propriété intellectuelle et droit à l'image 12
6.2. Préservation du secret et de la confidentialité 12
6.2.1. Règles générales 12
6.2.2. Chiffrement 13
6.3. Protection des données à caractère personnel 13
6.3.1. Devoirs des utilisateurs 13
6.3.2. Droits des utilisateurs 13

6.4. Enregistrements 14
6.4.1. Vidéoprotection 14
6.4.2. Enregistrements audio/visuels 14
6.4.3. Enregistrements téléphoniques 14

7. SECURITE ET VIGILANCE 14
7.1. Sécurité 14
7.2. Traçabilité 15
7.3. Filtrage 16
7.4. Scan Sécurité 16
7.5. Mesures d'urgence et plan de continuité d'activité 16
7.6. Perte ou vol 17

8. CONTROLE, MAINTENANCE ET GESTION DES RESSOURCES 17
8.1. Contrôle et audit 17
8.2. Maintenance 18
8.3. Consommations 19
8.4. Règles d'archivage électronique et de sauvegarde 19

9. DROITS ETENDUS 19

10. RESPONSABILITE ET SANCTIONS 20

11. DEROGATION 20

12. ENTREE EN VIGUEUR 21

GLOSSAIRE 22

1. PREAMBULE

La présente charte d'IFP Energies nouvelles (IFPEN) et de COFIP (ci-après « l'entreprise ») a pour objet de fixer les règles d'utilisation des systèmes d'information et de communication mis à la disposition des utilisateurs dans le cadre de leur activité professionnelle.

Les règles ainsi définies sont destinées à assurer un niveau optimal de sécurité, de confidentialité et de performance d'usage des systèmes d'information et de communication, en conformité avec les dispositions légales et réglementaires applicables ainsi qu'avec la jurisprudence des cours et tribunaux compétents.

Elle tient notamment compte des recommandations de la Commission nationale de l'informatique et des libertés (Cnil) et de celles de l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

La charte est rédigée dans le souci de concilier les intérêts de l'entreprise et de chaque utilisateur, qu'elle a pour objectif de responsabiliser dans l'usage qu'il fait des moyens informatiques qui sont mis à sa disposition. Elle manifeste ainsi la volonté de l'entreprise d'assurer un usage loyal, respectueux et responsable de ses systèmes d'information et de communication et de protéger son patrimoine et son image de marque.

La charte définit les règles mais ne couvre pas de façon exhaustive tous les cas de figure pratiques susceptibles de se présenter dans le cadre de l'utilisation des systèmes d'information et de communication mis à la disposition des utilisateurs. C'est dans l'esprit des règles ainsi édictées que chacun devra ajuster son comportement dans le cadre de situations non envisagées par le présent document.

La présente charte pourra évoluer en fonction du contexte légal et de la politique de sécurité applicable au sein de l'entreprise.

Pour une bonne application de la présente charte, l'utilisateur doit prendre connaissance du livret utilisateur, dont l'objet est de définir les termes utilisés dans la présente charte et de décliner au plan pratique les principes de mise en œuvre prévus par celle-ci.

2. PORTEE ET OPPOSABILITE

La présente charte est annexée au règlement intérieur applicable et produit, à ce titre, les mêmes effets. En conséquence, l'utilisateur est supposé en avoir pris connaissance.

La présente charte est indépendante de :

- La charte IFPEN pour l'exercice du droit à la déconnexion ;
- L'accord d'entreprise portant sur la mise en œuvre du télétravail ;
- L'accord d'entreprise portant sur l'exercice du droit syndical à IFPEN et sur la mise à disposition des technologies de l'information et de la communication auprès des organisations syndicales et du comité social et économique.

3. CHAMP D'APPLICATION

3.1. PERSONNES CONCERNEES

La charte est applicable, et donc opposable, aux catégories de personnels suivantes :

- toute personne contractuellement engagée auprès de l'entreprise et rattachée aux effectifs de cette dernière (CDI, CDD parmi lesquels doctorants, post-doctorants, contrats d'alternance, etc…) ;

- toute personne engagée par l'entreprise au titre d'un stage.

La présente charte est par ailleurs opposable aux catégories d'utilisateurs suivantes :

- le personnel des entreprises extérieures dès lors que ce personnel se voit tenu de respecter le règlement intérieur d'IFPEN et donc la présente charte qui y est annexée, et ce dans le cadre du contrat qui lie l'entreprise dont il relève à IFPEN ;

- les autres catégories de personnel externe dès lors que ce personnel se voit tenu de respecter le règlement intérieur d'IFPEN et donc la présente charte qui y est annexée, et ce dans le cadre du contrat qui le lie individuellement à IFPEN.

La charte peut être complétée de documents spécifiques à destination de certaines catégories de personnel. À ce titre, les administrateurs des systèmes d'information et de communication peuvent se voir opposer une charte administrateur qui précise les règles auxquelles ils sont assujettis et les droits dont ils bénéficient en cette qualité.

3.2. MOYENS CONCERNES

Sont visés par la présente charte :

- l'ensemble des systèmes d'information et de communication qui sont la propriété de l'entreprise et/ou qui sont mis à la disposition des utilisateurs à des fins professionnelles et/ou tout autre nouveau système susceptible d'être mis en place au sein de l'entreprise ;

- l'ensemble des systèmes d'information et de communication qui sont la propriété personnelle de l'utilisateur, et pour lesquels celui-ci a obtenu une autorisation d'utilisation dans le cadre de son activité professionnelle.

3.3. USAGES CONCERNES

La charte s'applique à tous les types d'usage des systèmes d'information et de communication de l'entreprise, quelle que soit leur fréquence, leur objectif ou leur périodicité et qu'ils aient lieu :

- dans les locaux de l'entreprise, ce qui s'entend de son siège social ainsi que de tous les lieux d'établissement quels qu'ils soient ;

- dans le cadre d'un accès distant hors de l'entreprise, quel que soit le lieu de cet accès (domicile de l'utilisateur, site d'un client, d'un fournisseur, espace de co-working, etc.).

4. CONDITIONS GENERALES D'UTILISATION

4.1. USAGE PROFESSIONNEL

Les systèmes d'information et de communication de l'entreprise, quelle que soit leur nature, sont réservés à un usage professionnel et sont donc présumés revêtir un caractère professionnel, et ce quelles que soient leurs conditions effectives d'utilisation.

Selon la jurisprudence constante en la matière, sont présumés avoir un caractère professionnel, notamment mais non exclusivement :

- les fichiers créés par un utilisateur grâce aux systèmes d'information et de communication de l'entreprise ou des moyens ou ressources mises à la disposition de ce dernier pour l'exécution de sa mission, sauf lorsque celui-ci les identifie comme étant « perso » ;

- les connexions établies par un utilisateur sur des sites internet pendant son temps de travail et pour l'exécution de sa mission grâce aux systèmes d'information et de communication de l'entreprise ;

- une clé USB et tout autre support matériel dès lors qu'elle est connectée à un outil informatique mis à la disposition de l'utilisateur par l'entreprise dans le cadre de son contrat de travail, que la clé USB ou ledit support soit la propriété de l'entreprise ou de l'utilisateur.

Il résulte du principe précité que :

- l'entreprise peut accéder à l'ensemble des éléments du système d'information et de communication précités hors la présence de l'utilisateur concerné ;

- aucune information à caractère professionnel ne peut être stockée dans un répertoire informatique utilisé à des fins non professionnelles ;

- aucune information à caractère professionnel ne peut être émise, reçue ou traitée sur des systèmes d'information et de communication non professionnels sans autorisation de l'entreprise.

L'utilisateur reconnaît en particulier que la messagerie professionnelle est par principe réservée à un usage professionnel et qu'elle ne doit pas en conséquence être utilisée dans un autre contexte. L'utilisateur s'interdit en conséquence de diffuser son adresse de messagerie électronique sur des services en ligne sans rapport avec l'activité professionnelle.

En outre, l'inscription sur une liste de diffusion (ou newsletter) requiert une autodiscipline de la part de l'utilisateur, qui doit s'assurer au préalable et de manière continue de la pertinence et de la nécessité d'une telle liste de diffusion ainsi que des conséquences d'une inscription à celle-ci à partir de son adresse email professionnelle (fréquence de réception des messages, poids des messages, encombrement des réseaux, etc.).

L'utilisateur reconnaît également que l'accès à des services en ligne et applications est également réservé à un usage professionnel.

4.2. USAGE NON PROFESSIONNEL

Bien que les systèmes d'information et de communication de l'entreprise soient réservés à un usage professionnel, leur utilisation à des fins non professionnelles est tolérée, pour répondre en cas d'urgence à des obligations socialement admises et/ou pour des usages raisonnables et résiduels.

L'utilisateur reconnaît que la tolérance de l'entreprise s'agissant de l'usage non professionnel des systèmes d'information et de communication pourra être limitée, voire suspendue en cas d'abus, c'est-à-dire si l'utilisateur n'a pas respecté les préconisations qui s'imposent en la matière tant en termes de temps passé que d'activités accomplies.

En outre, l'usage non professionnel des systèmes d'information et de communication de l'entreprise par l'utilisateur ne doit pas :

- perturber de quelque façon que ce soit le bon fonctionnement des systèmes d'information et de communication de l'entreprise ;
- compromettre les activités exercées au sein de l'entreprise et la continuité du service;
- porter atteinte aux obligations qui incombent à l'utilisateur vis-à-vis de l'entreprise ou des autres membres du personnel (dignité, loyauté, discrétion, neutralité, réserve) ;
- porter atteinte à l'entreprise ou être susceptible d'engager sa responsabilité ;
- poursuivre un quelconque but lucratif ;
- porter atteinte à l'image de marque ou à la réputation de l'entreprise.

L'usage non professionnel par l'utilisateur des systèmes d'information et de communication de l'entreprise se traduit dans les faits par :

- la possibilité de créer un répertoire ou dossier informatique non professionnel en local ou sur les serveurs mis à la disposition de l'utilisateur par l'entreprise ;
- de façon plus générale, la possibilité d'utiliser à des fins non professionnelles les différents outils mis à la disposition de l'utilisateur par l'entreprise (réseau internet, téléphonie fixe et mobile, messagerie instantanée, outils de messagerie, logiciel de traitement de texte, imprimante, etc.) dans les conditions précitées.

L'utilisateur est entièrement responsable de l'usage des systèmes d'information et de communication de l'entreprise à des fins privées et dégage en conséquence l'entreprise de toute responsabilité à ce titre.

Afin de garantir la confidentialité des répertoires, fichiers, contenus et messages électroniques non professionnels, il est impératif que l'utilisateur utilise le terme « perso », abréviation de « personnel » :

- dans le nom du répertoire informatique ;
  seuls les fichiers et dossiers stockés dans un répertoire identifié comme « perso » seront considérés comme non professionnels ;
- dans la zone objet du message électronique, auquel cas le tiers destinataire du message devra être informé de cet usage ;
- si le moyen de communication utilisé ne comporte pas de champ « objet » (messagerie instantanée, sms…), le message à caractère non professionnel doit débuter par le terme « perso ».

À défaut d'utiliser le terme « perso » comme décrit précédemment, tous les répertoires, fichiers et messages informatiques sont considérés comme professionnels.

Le caractère non professionnel de l'usage des systèmes d'information et de communication interdit par principe à l'entreprise d'accéder aux contenus ou données émis, reçus ou échangés dans ce cadre.

Toutefois, le caractère non professionnel du répertoire ou des courriers électroniques échangés, ne fait pas obstacle à ce que l'entreprise, par le biais d'un administrateur des systèmes d'information ou de toute autre personne habilitée, puisse accéder de manière exceptionnelle à ces éléments dans les hypothèses suivantes :

- lorsqu'il existe un risque avéré pour l'entreprise en termes notamment de sécurité, de continuité de service, ou un risque grave de voir sa responsabilité engagée, ce qui peut impliquer la mise en œuvre d'une procédure de quarantaine ou le cas échéant une suppression de l'élément considéré en cas de détection ou de suspicion de code malveillant ;
- dans le cadre de sa mission consistant à assurer le fonctionnement normal et la sécurité des systèmes d'information et de communication, ce qui se réfère notamment à la mise en œuvre

d'une opération de maintenance, d'une procédure de conservation technique (sauvegarde, plan de continuité ou de reprise d'activité) ;
- dans tous les autres cas et pour des motifs légitimes en présence de l'utilisateur ou ce dernier dûment appelé, ou, en son absence, dès lors que l'entreprise y est autorisée par une décision de justice ou de toute autorité habilitée à cet effet (police, gendarmerie, douanes, Cnil, Direction générale de la concurrence, de la consommation et de la répression des fraudes…).

Que ce soit à titre professionnel ou non professionnel, il est rappelé à l'utilisateur qu'il est formellement interdit de se connecter sur des sites à caractère pornographique, pédopornographique, injurieux, violent, raciste, antisémite ou nazi, d'incitation à la haine ou à la violence ou à la commission d'acte illicite, discriminatoire, diffamatoire, faisant l'apologie du terrorisme, contrefaisant, ou manifestement contraire à l'ordre public ou de télécharger ou visionner ou stocker ou transmettre, etc. des contenus de telle nature.

4.3. CONDITIONS D'ACCES ET D'IDENTIFICATION

4.3.1. Principes généraux relatifs à la gestion des droits d'accès

Chaque utilisateur est doté d'un ou de plusieurs moyens d'authentification permettant l'accès aux systèmes d'information et de communication. Ces moyens d'authentification peuvent reposer sur les dispositifs suivants, décrits dans le livret utilisateur si l'entreprise y a recours :

- identification par attribution d'un identifiant et d'un mot de passe,
- solution OTP (one time password),
- identification physique (badge, carte à puce),
- identification par l'intermédiaire d'un dispositif biométrique,
- identification par l'usage de certificats électronique ou signature électronique,
- autres modes d'identification le cas échéant.

Les moyens d'authentification sont confidentiels.

Par conséquent, l'utilisateur s'interdit d'adopter les comportements suivants :

- procéder à la moindre divulgation, même intra-service, de son ou de ses moyens d'authentification ;
- utiliser un moyen d'authentification d'un autre utilisateur, dans l'hypothèse où il en aurait eu connaissance ;
- supprimer, masquer ou modifier son identité ou son identifiant ;
- user de son droit d'accès pour accéder à des applications, à des données ou à un compte informatique autres que ceux qui lui auront été éventuellement attribués ou pour lesquels il a reçu une autorisation d'accès de la part de la Direction du système d'information ;
- lorsqu'un accès distant lui est accordé, utiliser d'autres moyens d'authentification que ceux qui lui ont été remis à cet effet.

Les mots de passe doivent être modifiés selon une fréquence déterminée et fixée le cas échéant dans le livret utilisateur. L'utilisateur s'engage en outre à suivre toutes les prescriptions complémentaires susceptibles de lui être signifiées afin d'assurer la sécurité et la confidentialité des mots de passe.

Tout usage des systèmes d'information et de communication est réputé avoir été réalisé par le bénéficiaire du moyen d'authentification qui en assume toute conséquence, notamment sur un plan juridique et financier, sauf à ce que celui-ci ait engagé préalablement une demande de suspension ou de suppression d'autorisation, ou soit en mesure de démontrer le contraire.

4.3.2. Modification / suspension des accès

En cas de suspicion de compromission de ses moyens d'authentification, l'utilisateur est tenu d'en aviser sans délai la Direction du système d'information, ou le cas échéant de suivre la procédure formalisée dans le livret utilisateur. A défaut d'avoir procédé à cette information, l'utilisateur demeurera considéré comme étant à l'origine des actes réalisés sur les systèmes d'information et de communication avec ses moyens d'identification. Seul le respect de la procédure d'information précitée sera de nature à dégager la responsabilité de l'utilisateur pour les agissements qui auraient lieu post-déclaration sous son identité.

L'étendue des droits d'accès aux systèmes d'information et de communication accordés à toute personne est déterminée par l'entreprise et pourra être adaptée à sa seule initiative.

L'entreprise aura par ailleurs la possibilité de suspendre temporairement, si elle l'estime nécessaire, le droit accordé à toute personne d'accéder à ses systèmes d'information et de communication.

4.4. GESTION DES ABSENCES ET DES DEPARTS

Chaque utilisateur doit veiller à ce que la continuité du service soit assurée, conformément aux modalités d'organisation définies par l'entreprise.

En cas d'absence ou de départ de l'utilisateur, l'entreprise se réserve le droit de mettre en place une solution de routage des messages électroniques ou toute autre solution technologique permettant d'assurer la continuité de l'activité de l'entreprise.

En cas d'absence de l'utilisateur, pour quelque raison et durée que ce soit, l'entreprise se réserve le droit d'accéder directement aux différents dossiers, répertoires, courriers électroniques professionnels et plus généralement tout document à caractère professionnel de l'utilisateur, ayant recours en tant que de besoin, aux administrateurs des systèmes d'information.

À l'annonce du départ de l'entreprise d'un utilisateur, et pour des raisons légitimes de protection des intérêts de l'entreprise, les droits d'accès et les conditions d'utilisation des systèmes d'information et de communication pourront être modifiés et des règles particulières de traçabilité pourront être mises en œuvre.

Lors de son départ, l'utilisateur doit :

- remettre en bon état général de fonctionnement l'ensemble des systèmes d'information et de communication auxquels il lui a été donné accès par l'entreprise ;
- restituer tous les moyens d'authentification et d'accès qui lui ont été fournis par l'entreprise ;
- supprimer la veille de son départ le répertoire et les messages électroniques nommés « perso », ainsi que tous les documents de même nature. À défaut, et sauf procédure judiciaire ou enquête administrative, ces éléments sont supprimés au départ de l'utilisateur de l'entreprise, (en dehors des sauvegardes) sans être consultés et sans qu'aucune copie ne soit réalisée.

Sauf nécessité liée à la continuité du service et pour une durée raisonnable qui peut dépendre de la fonction de la personne, le compte messagerie de l'utilisateur, ainsi que ses moyens d'authentification, sont désactivés à son départ.

5. CONDITIONS SPECIFIQUES D'UTILISATION

5.1. MOBILITE ET ACCES DISTANT

Dans le cadre de ses déplacements professionnels, quelle que soit leur durée ou leur fréquence, l'utilisateur assure la garde et la responsabilité des systèmes d'information et de communication auxquels il est susceptible d'accéder à distance et des matériels mis à sa disposition pour ce faire.

Dans la mesure où l'utilisation « nomade » de ces matériels et l'accès à distance aux systèmes d'information et de communication de l'entreprise impose à l'utilisateur un niveau de surveillance et de confidentialité renforcé, ce dernier s'engage à adopter une attitude de prudence et de réserve au regard des informations, données et ressources qu'il pourrait être amené à consulter, manipuler ou à échanger dans un tel contexte.

L'utilisateur doit également veiller à ce que des tiers non autorisés ne puissent accéder aux systèmes d'information et de communication de l'entreprise et à leurs contenus.

En cas d'incident avéré ou de doute, l'utilisateur doit immédiatement en aviser la Direction du système d'information.

5.2. PRET DE MATERIEL INFORMATIQUE OU TELEPHONIQUE

En complément des moyens informatiques mis à disposition de l'utilisateur à son arrivée pour la durée de son contrat de travail, l'entreprise prête également du matériel pour des périodes de courte durée (quelques jours) ou de moyenne durée (exemple : mission en France ou à l'étranger).

L'utilisateur s'engage à restituer les matériels informatique ou téléphonique qui lui sont prêtés par l'entreprise à titre provisoire, ceci à la fin de la période de prêt et sans délai.

5.3. TELETRAVAIL

La mise en œuvre du télétravail fait l'objet d'un accord d'entreprise dédié à cet effet.

Sauf disposition particulière décrite dans l'accord d'entreprise, la charte des SI s'applique également en télétravail.

5.4. MATERIEL PERSONNEL UTILISE A DES FINS PROFESSIONNELLES

L'utilisateur n'est pas autorisé à utiliser à des fins professionnelles des systèmes d'information et de communication qui sont sa propriété personnelle ou qu'il détient à titre personnel, sauf à avoir obtenu une autorisation de l'entreprise et sous réserve du respect des prescriptions techniques exigées par la Direction du système d'information.

5.5. GESTION DES CONNAISSANCES ET DE L'ESPACE COLLABORATIF

L'entreprise privilégie, autant que faire se peut, le partage et la capitalisation des connaissances, et peut à ce titre mettre en place des espaces collaboratifs de travail.

Chaque utilisateur s'engage à être attentif à la pertinence et à la qualité des informations diffusées au sein de ces espaces collaboratifs et à travers les outils de gestion des connaissances mis à sa disposition.

Par souci de qualité, de responsabilité et de protection du patrimoine informationnel de l'entreprise, l'utilisation de ces mêmes espaces et outils peut faire l'objet d'opérations de contrôle, d'audit, de modération et de traçabilité renforcées.

Aux mêmes fins, l'entreprise a mis en place des outils de marquage de tout ou partie des éléments des bases de données constituées dans ce cadre, pour éviter toute extraction. Les utilisateurs seront avertis de la présence de tels outils.

5.6. MEDIAS SOCIAUX

L'entreprise estime que les réseaux sociaux extérieurs à l'entreprise occupent une place grandissante dans la vie professionnelle dans la mesure où ils permettent aux utilisateurs de créer de nouvelles relations professionnelles et d'optimiser les échanges professionnels autour de leurs projets.

Cependant, l'utilisation des réseaux sociaux peut être source de risques et de responsabilité notamment en termes d'image ou de fraude. Aussi, afin de limiter les risques encourus, les règles suivantes ont été arrêtées.

5.6.1. Usage professionnel

L'utilisateur est autorisé à utiliser un ou plusieurs réseaux sociaux qui s'avèrent nécessaire dans le cadre de son activité professionnelle et respecter les règles suivantes :

- s'abstenir de publier un contenu de façon anonyme et s'identifier clairement en précisant sa fonction au sein de l'entreprise ;
- respecter l'entreprise, ne pas porter atteinte à sa sécurité, son image ou sa réputation ;
- répondre aux contributions des tiers avec pertinence, exactitude, en s'efforçant de promouvoir l'image de l'entreprise ;
- respecter les conditions générales d'utilisation du réseau social et l'ensemble des lois applicables (notamment en matière de concurrence, de consommation et de propriété intellectuelle, de droit de la presse, de propos illicites) ;
- utiliser uniquement les outils de communication de l'entreprise, selon les instructions qui lui ont été données et dans la perspective de valoriser l'entreprise ;
- s'abstenir de diffuser toute information confidentielle ou toute information commerciale sensible relative à l'entreprise, à ses partenaires ou à ses concurrents ;
- s'abstenir de favoriser des actes de concurrence de la part de tiers ;
- s'abstenir de consulter ou d'utiliser tout réseau social illicite ;
- plus généralement, prendre toutes les précautions utiles pour que l'utilisation des réseaux sociaux intervienne sans danger pour les systèmes d'information et de communication de l'entreprise.

L'usage des réseaux sociaux s'inscrit en tout état de cause dans le respect des règles et des bonnes pratiques établies par l'entreprise en matière de communication.

5.6.2. Usage non professionnel

Dans le cadre de la sphère non professionnelle et hors les murs de l'entreprise, l'utilisateur est bien évidemment libre d'utiliser les réseaux sociaux et d'y faire mention de son appartenance à l'entreprise. Cependant, il ne doit pas y avoir d'ambigüité sur le fait qu'il s'y exprime en son nom propre ; il ne doit pas émettre d'opinion qui implique l'entreprise ; il ne doit pas utiliser sans autorisation les éléments graphiques qui font l'identité et l'image de celle-ci ; il s'interdit de communiquer la moindre information sur son activité professionnelle, en particulier des informations

confidentielles, des informations commerciales sensibles relatives à l'entreprise, à ses partenaires ou à ses concurrents, des informations relatives aux conditions de travail, à l'organisation générale, au calendrier d'évènements, à la rémunération, etc.

5.6.3. Signalement

Qu'il utilise les réseaux sociaux à titre professionnel ou non professionnel, l'utilisateur pourra informer l'entreprise d'un agissement de tiers dont il aurait connaissance et qui serait susceptible de porter atteinte à la réputation de l'entreprise ou à un droit de ce dernier, notamment un droit de propriété intellectuelle quel qu'il soit.

6. PROTECTION DE LA PROPRIETE INTELLECTUELLE, DES INFORMATIONS ET DES DONNEES

6.1. PROPRIETE INTELLECTUELLE ET DROIT A L'IMAGE

L'utilisation des systèmes d'information et de communication de l'entreprise implique le respect des droits de propriété intellectuelle et du droit à l'image.

Sans que cette liste soit exhaustive, l'utilisateur s'engage à :

- utiliser les logiciels et applications, dans les conditions de la licence souscrite par l'entreprise ;
- ne pas effectuer de copie illicite de logiciel ou d'applications et, a fortiori, ne pas tenter d'installer des logiciels ou applications pour lesquels l'entreprise ne possèderait pas un droit d'usage ;
- ne pas reproduire, copier, utiliser remettre à des tiers ou diffuser, les bases de données, pages web, dessins, modèles, logos ou autres créations de l'entreprise ou de tiers protégés par le droit d'auteur ou un droit privatif, sans avoir obtenu préalablement l'autorisation du titulaire de ces droits ;
- ne pas reproduire, copier ou diffuser des textes, des images, des photographies, des œuvres musicales, audiovisuelles ou multimédia et, plus généralement, toute création ou invention provenant du réseau internet, d'applications web ou mobiles ;
- ne pas reproduire, copier, utiliser ou diffuser des éléments susceptibles de porter atteinte à l'image ou à la vie privée des utilisateurs ou de tiers à l'entreprise.

6.2. PRESERVATION DU SECRET ET DE LA CONFIDENTIALITE

6.2.1. Règles générales

La sauvegarde des intérêts de l'entreprise nécessite le respect par l'utilisateur d'une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations, des données et des productions de toute nature, dont l'IFPEN est ou non à l'initiative, et dont il a connaissance dans le cadre de l'exercice de son activité professionnelle.

Par ailleurs, le respect de la confidentialité des données est une exigence essentielle de l'entreprise dans la mesure où elle est soumise à des obligations particulières en termes de secret des affaires et de confidentialité et est à ce titre susceptible d'être exposée à des risques spécifiques.

Le respect de cette obligation implique notamment de :

- être vigilant sur les droits d'accès qu'il donne aux autres utilisateurs et veiller à ce que les tiers non autorisés n'aient pas connaissance de telles informations et données ;
- n'accéder qu'aux informations et données en rapport direct avec sa fonction et ne pas chercher, en conséquence, à prendre connaissance d'informations et données réservées à d'autres utilisateurs ;
- ne pas extraire ces informations et données confidentielles et ne pas les reproduire sans l'accord préalable du supérieur hiérarchique et/ou les détourner de leur utilisation normale à des fins non professionnelles ;
- d'une manière générale, respecter les règles d'éthique professionnelle, de déontologie, ainsi que les obligations de réserve et devoir de discrétion en usage au sein de l'entreprise.

La diffusion de toute information ou donnée ne peut être réalisée qu'aux conditions suivantes :

- habilitation de l'émetteur ;
- désignation d'un destinataire autorisé ;
- respect d'une procédure sécurisée.

En fonction du niveau de confidentialité appliqué à ces informations, l'utilisateur doit notamment éviter de les communiquer ou les transporter sans protection (chiffrement) via des supports non fiabilisés (messagerie, clés USB, ordinateurs portables, disques externes, etc.), et ne pas les déposer ni les sauvegarder sur un serveur externe ou ouvert au grand public.

6.2.2. Chiffrement

L'usage d'outils ou de solutions de chiffrement est encouragé notamment pour protéger des données sensibles (brevets notamment) ou les matériels nomades (ordinateurs portables). Les modalités pratiques du recours au chiffrement sont définies dans le livret utilisateur.

L'usage d'outils ou de solutions de chiffrement ne doit cependant pas :

- nuire au bon fonctionnement de l'entreprise et à l'accès permanent aux contenus à caractère professionnel ; au départ du collaborateur tous les contenus chiffrés doivent pouvoir être librement accessibles ;
- avoir pour objet ou pour effet de dissimuler des contenus privés illicites.

6.3. PROTECTION DES DONNEES A CARACTERE PERSONNEL

6.3.1. Devoirs des utilisateurs

Les utilisateurs sont informés de la nécessité de respecter les dispositions légales en matière de traitements automatisés ou manuels de données à caractère personnel, prévues pour l'essentiel dans le Règlement (UE) 2016-679 du 27 avril 2016 entré en vigueur le 25 mai 2018 dit « Règlement général sur la protection des données » (RGPD) et la loi n°78-17 dite « Informatique et libertés » du 6 janvier 1978 dans sa version actualisée.

Dans ce cadre, les utilisateurs amenés à mettre en œuvre un traitement de données à caractère personnel devront se conformer à la procédure en vigueur telle que prévue dans le livret utilisateur et, s'il y a lieu, aux codes ou chartes de bonne conduite établis en matière de protection des données.

6.3.2. Droits des utilisateurs

L'entreprise met en œuvre des traitements de données à caractère personnel concernant les utilisateurs dans le respect de la règlementation applicable, en l'occurrence le Règlement (UE) 2016-679 du 27 avril 2016 entré en vigueur le 25 mai 2018 dit « Règlement général sur la protection des données » (RGPD) et la loi n°78-17 dite « Informatique et libertés » du 6 janvier 1978 dans sa version actualisée.

Nous vous invitons à prendre connaissance de la note d'information relative à la protection des données à caractère personnel des salariés qui vous a été communiquée et qui est accessible sur l'intranet et sur simple demande auprès du délégué à la protection des données à l'adresse DPO@ifpen.fr.

6.4. ENREGISTREMENTS

6.4.1. Vidéoprotection

Les utilisateurs sont informés de la mise en place d'un dispositif de vidéosurveillance dans les locaux de l'entreprise à des fins de sécurité et de prévention des atteintes aux biens et/ou aux personnes.

L'enlèvement ou la neutralisation de tout ou partie de ce dispositif de vidéosurveillance sans justificatif sont strictement interdits.

6.4.2. Enregistrements audio/visuels

Dans le cadre professionnel et dans l'objectif d'atteindre une certaine qualité de service, des outils techniques d'enregistrements vidéo et sonores sont susceptibles d'être mis en place.

Peuvent être soumis à des enregistrements notamment les web-conférences, les visio-conférences et les conférences téléphoniques.

Les utilisateurs sont informés de l'existence de ces outils d'enregistrement et du fait qu'ils sont activés par défaut sans qu'il soit besoin de le rappeler systématiquement à l'utilisateur. Ces enregistrements n'ont pas vocation à faire l'objet d'une exploitation publique. Si tel devait être le cas les personnes concernées se verront proposer de signer une autorisation spécifique.

6.4.3. Enregistrements téléphoniques

Par principe, et sauf autorisation préalable des personnes concernées, l'enregistrement des conversations téléphoniques est strictement interdit par la loi.

7. SECURITE ET VIGILANCE

7.1. SECURITE

Les systèmes d'information et de communication sont exclusivement installés, configurés et paramétrés par le personnel habilité par l'entreprise.

Lorsqu'il s'agit de moyens personnels de l'utilisateur, ceux-ci sont nécessairement autorisés voire contrôlés par ce même personnel.

À des fins de précaution, certaines configurations peuvent être verrouillées par l'entreprise (poste de travail, accès internet, etc.).

La mise en place d'outils de sécurité par l'entreprise ne dispense pas les utilisateurs d'une obligation de vigilance.

En effet, tout utilisateur a la charge, à son niveau, de contribuer à la sécurité des systèmes d'information et de communication mis à sa disposition, principalement en évitant l'introduction de codes malveillants susceptibles d'endommager le système d'information de l'entreprise ou en évitant les fuites de données.

Il en résulte que chaque utilisateur doit se former aux techniques de sécurité informatique et maintenir son niveau de connaissance en utilisant les outils mis à sa disposition par l'entreprise.

Au titre de cette obligation de vigilance, l'utilisateur doit se conformer notamment, mais non limitativement, aux règles suivantes :

- ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes d'information et de communication ou aux réseaux à travers les matériels dont il a usage ;
- ne pas utiliser ou tenter d'utiliser des comptes autres que ceux qui lui sont attribués ou tenter de masquer son identité ;
- ne pas effectuer des opérations susceptibles de nuire aux relations internes ou externes de l'entreprise ;
- ne pas désinstaller les outils et moyens de sécurité du système d'information ;
- appliquer les recommandations de sécurité et notamment se conformer aux dispositifs mis en place par la Direction du système d'information pour lutter contre les codes malveillants et les attaques par programmes informatiques ;
- protéger ses données professionnelles en les stockant directement sur des zones réseaux ou en utilisant les moyens de sauvegarde mis à disposition par la Direction du système d'information ;
- assurer la protection de ses informations et plus particulièrement celles considérées comme confidentielles. En particulier, ne pas transporter sans protection (telle qu'un chiffrement) des données sensibles sur des supports non fiabilisés tels que clés USB, disques externes, etc. ;
- veiller à verrouiller sa session en quittant son poste de travail (ou un poste en libre-service) ;
- signaler à la Direction du système d'information toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

En cas de réception de messages non sollicités, l'utilisateur veille à :

- ne pas ouvrir les pièces jointes ni cliquer sur les liens hypertextes ;
- ne pas y répondre ;
- ne pas le transférer ;
- informer la Direction du système d'information ;
- agir sur instruction de cette dernière.

7.2. TRAÇABILITE

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité à apporter la preuve, le cas échéant, du bon usage des systèmes d'information et de communication mis à la disposition des utilisateurs, l'entreprise se réserve le droit de mettre en œuvre des outils de traçabilité tels que des journaux de connexions de l'ensemble des systèmes d'information et de communication.

Le cas échéant, les traces informatiques sont conservées pour une durée limitée telle que figurant dans le registre des traitements.

Ces traces peuvent faire l'objet d'un traitement statistique.

Ces traces peuvent être fournies aux autorités compétentes selon les dispositions légales et réglementaires en vigueur.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

7.3. FILTRAGE

Pour satisfaire aux obligations légales qui lui incombent, tenant à sa capacité de tenter de prévenir tout usage illicite de ses systèmes d'information et de communication l'entreprise se réserve le droit de mettre en place des outils de filtrage permettant d'analyser les conditions d'utilisation de ces moyens, d'interdire tel ou tel protocole, ou encore de restreindre certaines catégories de sites internet ou d'applications.

Ces outils, en ce qu'ils portent entre autres sur l'accès à internet, permettent un contrôle des connexions des utilisateurs.

Tout détournement, altération ou modification de ces outils ou des données recueillies grâce à ces outils est strictement interdit.

7.4. SCAN SECURITE

Le scan sécurité consiste à détecter au plus tôt à travers des outils informatiques la présence de codes malveillants dans les systèmes d'information et de communication de l'entreprise ainsi que la perte ou la fuite de données sensibles.

Il permet de disposer d'un dispositif d'alerte prudentiel et rapide pour améliorer la sécurité des systèmes d'information.

L'entreprise se réserve le droit de mettre en œuvre des opérations de scan sécurité de ses systèmes d'information et de communication tels que les documents, les dossiers, les courriers électroniques, pièces jointes, fichiers, etc.

La liste des signatures virales et des séquences recherchées par les outils de scan sécurité est déterminée par l'entreprise. Elle n'est pas accessible ni communiquée aux utilisateurs dans la mesure où elle dépend de la politique de sécurité de l'entreprise.

7.5. MESURES D'URGENCE ET PLAN DE CONTINUITE D'ACTIVITE

L'utilisateur est informé qu'en cas de sinistre, d'incident majeur ou de nécessité impérative, l'entreprise peut mettre en œuvre un certain nombre de mesures exceptionnelles visant à assurer la continuité de son activité et le respect de ses engagements contractuels ou légaux.

Dans cette hypothèse, l'utilisateur pourra être amené, à la demande de l'entreprise, à prendre des mesures d'urgence et de sécurité spécifiques, qu'il s'engage à appliquer sans délai.

Ces mesures exceptionnelles peuvent inclure, notamment, une dégradation de service sur tout ou partie des ressources du système d'information (temps de réponse, capacité de stockage, d'accès ou de traitement de l'information, etc.), la suppression temporaire de l'accès à certaines ressources du système d'information (messagerie, connexion internet, accès applicatifs, éléments relatifs au poste de travail, etc.) ou la mise en œuvre de contraintes exceptionnelles (restriction temporaire de l'accès au site ou au système d'information, télétravail, déplacement sur des sites de secours tiers, etc.).

7.6. PERTE OU VOL

L'utilisateur est tenu d'informer, sans délai, la direction compétente telle que définie dans le livret utilisateur de tout dysfonctionnement, altération, perte, vol, destruction et autre événement susceptible d'affecter les systèmes d'information et de communication.

Il est tenu, en particulier, de signaler à l'entreprise toute tentative d'intrusion extérieure, de falsification ou de présence de virus.

Ceci s'applique aussi bien au matériel mis à sa disposition (ordinateur portable, mobile, dispositif de stockage de données, autres matériels) ainsi qu'aux moyens d'accès et d'authentification (badges, cartes, autres tokens…).

L'utilisateur devra, selon les cas, soit assister l'entreprise, soit procéder lui-même à toutes les démarches rendues nécessaires à la suite d'un incident de quelque nature que ce soit (déclaration d'assurance, dépôt de plainte, etc.).

8. CONTROLE, MAINTENANCE ET GESTION DES RESSOURCES

8.1. CONTROLE ET AUDIT

Les opérations de contrôle et d'audit portent sur la régularité de l'utilisation des systèmes d'information et de communication. Elles se justifient par les obligations incombant à l'entreprise.

En effet, du fait de son activité, l'entreprise est soumise à une obligation générale de sécurité, en application des dispositions du Code pénal relatives à la protection des systèmes de traitement automatisés de données, et de la règlementation applicable en matière de protection des données à caractère personnel.

L'entreprise, en tant qu'employeur, dispose également d'un pouvoir de contrôle de l'activité des utilisateurs et en particulier, le respect par ces derniers de la présente charte.

L'utilisation des systèmes d'information et de communication pourra faire l'objet d'une surveillance afin de détecter toute utilisation non conforme, d'optimiser cette même utilisation ou encore de mener des analyses statistiques.

L'entreprise se réserve ainsi le droit, notamment :

- de vérifier le trafic informatique entrant et sortant et le trafic transitant sur le réseau interne ;
- de diligenter des audits pour vérifier que les consignes d'usage et les règles de sécurité et de sûreté sont appliquées par l'utilisateur sur les ressources du système d'information ;
- de contrôler l'origine licite des logiciels installés sur les systèmes d'information ;
- de conserver des fichiers de journalisation des traces en fonction des besoins propres de chaque système d'information ;
- de transmettre aux autorités judiciaires sur requête tout ou partie des enregistrements disponibles.

En outre, en cas d'incident, l'entreprise se réserve le droit de :

- surveiller le contenu des informations qui transitent sur son système d'information ;
- vérifier le contenu stocké sur les ressources du système d'information attribuées aux utilisateurs ;
- procéder à toutes copies utiles pour faire valoir ses droits.

Ces opérations de contrôle et d'audit relèvent des compétences de la Direction du système d'information, qui a la charge de la qualité, de la protection et de la sécurité des systèmes d'information et de communication fournis aux utilisateurs.

En particulier, dans le cadre de ses fonctions, la Direction du système d'information exerce un contrôle notamment des durées de connexion et des sites les plus visités. En cas de perturbation induite par l'apparition intempestive d'alertes suite à des tentatives d'infection des systèmes à l'aide de virus informatiques, elle est habilitée à mener toutes les investigations qu'elle jugera utiles aux fins d'éradiquer lesdits virus.

Tout intervenant en charge de contrôles ou d'audit doit impérativement respecter la confidentialité des échanges électroniques et des fichiers des utilisateurs.

Les utilisateurs sont toutefois informés que les administrateurs des systèmes d'information sont conduits, du fait de leurs fonctions, à avoir accès à l'ensemble des informations des utilisateurs (fichiers, messages, connexions à internet, etc.), professionnelles et personnelles, y compris à celles qui sont enregistrées sur leur poste de travail.

Néanmoins, ces administrateurs des systèmes d'information sont tenus au secret professionnel et ne peuvent utiliser leurs droits qu'à des fins strictement professionnelles.

En cas de faisceau d'indices laissant supposer qu'un utilisateur met en cause les intérêts et la sécurité de l'entreprise en ne respectant pas les règles instituées par la charte, la Direction du système d'information se réserve le droit d'alerter la Direction des ressources humaines.

En cas de non-respect avéré de la présente charte par un utilisateur, la Direction du système d'information se verra dans l'obligation d'avertir le supérieur hiérarchique de l'utilisateur afin que celui-ci décide des suites éventuelles à donner à cette procédure. Suivant la gravité des faits, les droits d'accès de l'utilisateur concerné pourront être suspendus temporairement ou définitivement.

Tout matériel, logiciel ou application installés illicitement seront supprimés ou désactivés par la Direction du système d'information dès le constat de leur présence sur le poste de travail, ou matériel nomade, ou de leur accessibilité.

8.2. MAINTENANCE

La mise à disposition des systèmes d'information et de communication implique nécessairement des opérations de maintenance technique (maintenance corrective, maintenance préventive ou évolutive), pour assurer leur bon fonctionnement et la sécurité associée à leur utilisation.

Ces opérations prennent la forme d'une intervention d'une « personne habilitée » soit sur site, soit à distance.

Dans le cas où l'opération de maintenance nécessite « une prise en main à distance » sur le poste ou le matériel nomade de l'utilisateur par la « personne habilité », l'utilisateur devra explicitement autoriser cette action.

Dans ce cadre, la « personne habilitée » peut être amenée à prendre connaissance de l'ensemble des éléments présents sur le poste ou le matériel nomade de l'utilisateur qu'il s'agisse d'un usage professionnel ou privé.

Si, à l'occasion d'opérations de maintenance, une utilisation anormale et/ou un contenu illicite ou préjudiciable sont identifiées, l'entreprise en tirera les conséquences qui s'imposent.

Il est rappelé que l'utilisateur ne doit en aucun cas communiquer ses moyens d'identification et d'authentification, mêmes pour des opérations de maintenance.

8.3. CONSOMMATIONS

Pour la bonne gestion des ressources liées aux systèmes d'information et de communication, un suivi des consommations de chaque utilisateur est réalisé :

- pour les impressions, le suivi des consommables (nombre de pages imprimées, date, heure, etc.) est fourni par le dispositif de gestion des copieurs multifonctions ;
- pour la téléphonie fixe et mobile, le contrôle des consommations (numéros appelés, date, heure, durée, coût) peut être effectué sur la base des factures détaillées des opérateurs de téléphonie ;
- pour les systèmes d'information et de communication nomades, les éléments de la communication (site internet, date, heure, durée, volume) sont disponibles via les opérateurs internet, à travers les services de suivi des consommations qu'ils proposent.

Les informations ainsi disponibles, qui sont principalement dédiées à l'analyse des consommations, peuvent, en tout état de cause, être utilisées pour démontrer toute utilisation contrevenante aux obligations, droits et devoirs prévus dans la présente charte ou pour servir de preuve d'un fait manifestement excessif ou illicite.

8.4. REGLES D'ARCHIVAGE ELECTRONIQUE ET DE SAUVEGARDE

Chaque utilisateur doit mettre en œuvre et organiser, selon les instructions de sa hiérarchie, les moyens nécessaires à la conservation (également appelé archivage) des messages, des informations et des données de toute nature lorsque cela est nécessaire.

L'utilisateur est dans l'obligation de respecter la politique de conservation et d'archivage mise en œuvre au sein de l'entreprise.

L'utilisateur est responsable de ses données professionnelles. Il veillera tout particulièrement à les placer dans les emplacements protégés, sauvegardés automatiquement, mis à disposition par la Direction du système d'information.

L'utilisateur est également responsable de ses données personnelles, doit s'assurer de la sauvegarde de celles-ci, et être vigilant sur les droits d'accès qu'il donne aux autres utilisateurs sur celles-ci.

9. DROITS ETENDUS

Certains utilisateurs peuvent disposer de « droits étendus », c'est-à-dire de droits particuliers sur leur poste de travail, accordés par la Direction du système d'information.

Il peut s'agir de droit divers : installation, désinstallation, paramétrage simple ou avancé, ... sans que cette liste ne soit exhaustive.

L'utilisateur qui se voit accorder des droits étendus est pleinement responsable de ses agissements et ne doit pas agir en dehors des droits et autorisations qui lui ont été accordés. L'activation de ces droits est conditionnée par l'acceptation des conditions particulières proposées à l'utilisateur lors de sa demande. La demande d'activation des droits étendus est tracée.

En cas de non-respect des conditions particulières liées à l'usage de droits étendus ou de risque de mise en danger du système d'information, la Direction du système d'information se réserve le droit de retirer les droits étendus qu'il aura accordés à un utilisateur.

En cas de panne logicielle bloquant le poste de travail liée à l'usage de droits étendus, la Direction du système d'information ne sera pas en mesure de pratiquer des analyses détaillées et se limitera à une réinstallation dans une configuration standard.

La réinstallation des logiciels non fournis par la Direction du système d'information reste à la charge de l'utilisateur.

Le présent article ne s'applique pas aux administrateurs des systèmes d'information dont les interventions relèvent de la « charte administrateur ».

10. RESPONSABILITE ET SANCTIONS

L'utilisateur est responsable :

- dans le cadre de son activité professionnelle, de l'utilisation des systèmes d'information et de communication en conformité avec la présente charte ;
- dans la sphère de sa vie privée résiduelle, seul, à l'exclusion donc de toute responsabilité de l'entreprise, de tout usage effectué à caractère non professionnel.

En cas de manquement grave d'un utilisateur à l'une des dispositions de la présente charte, la Direction du système d'information en rend compte immédiatement à la Direction des ressources humaines en communiquant les éléments de preuve nécessaires.

Toute mauvaise utilisation ou utilisation non conforme aux conditions et limites définies par cette charte est constitutive d'une faute.

En conséquence, le non-respect des dispositions légales et règlementaires et des dispositions de la présente charte expose l'utilisateur en cause à des sanctions disciplinaires, prévues dans le règlement intérieur, et/ou à des poursuites judiciaires.

En outre, l'utilisateur s'expose à des restrictions d'usage concernant son droit d'utiliser les systèmes d'information et de communication, notamment le contrôle renforcé, la suspension, le blocage, le retrait voire la suppression pure et simple de son droit d'utiliser tout ou partie des systèmes d'information et de communication, de sites web et des applications, voire l'exclusion.

L'entreprise, pour sa part, déclare mettre en œuvre, par le biais notamment de la présente charte, tous les efforts nécessaires à un bon usage des systèmes d'information et de communication.

11. DEROGATION

Toute demande de dérogation temporaire aux dispositions de la présente charte doit être présentée, par écrit, à la Direction du système d'information, qui se réserve le droit de l'accepter ou de la refuser et d'en prévoir les conditions et modalités.

L'entreprise peut définir des règles dérogatoires individuelles ou collectives si des circonstances exceptionnelles l'exigent.

12. ENTREE EN VIGUEUR

Afin de conférer à la présente charte le statut d'annexe au règlement intérieur conformément à l'article L.1321-5 du Code du travail, l'entreprise a suivi la procédure prévue par le Code du travail relative à l'opposabilité et à l'entrée en vigueur du règlement intérieur.

À ce titre, l'entreprise a respecté les obligations qui lui incombent, qui consistent en l'occurrence à informer et consulter le Comité social et économique central (CSEC), à publier la présente charte par voie d'affichage sur des médias numériques, à en déposer un exemplaire au greffe du Conseil de prud'hommes de son ressort et à en communiquer deux exemplaires à l'Inspection du travail.

La présente charte entrera en vigueur un mois après les formalités précitées accomplies et aura la même valeur juridique que le règlement intérieur.

En cas de contradiction entre les termes de la charte des systèmes d'information et le règlement intérieur, les dispositions de la présente charte primeront.

GLOSSAIRE

Au sens de la présente charte, les termes ci-dessous ont la signification suivante :

- « administrateur des systèmes d'information » : personne dont l'emploi ou la fonction lui confère des droits d'accès privilégiés sur tout ou partie des systèmes d'information de l'entreprise ;

- « application » : programme destiné à traiter une tâche donnée pour les besoins particuliers de l'utilisateur et les programmes exécutables associés, accessible via le réseau internet ou de télécommunication ;

- « charte » : le présent document et les annexes susceptibles d'y être jointes constituant la charte des systèmes d'information de l'entreprise ;

- « code malveillant » : logiciel développé dans le but de nuire à un système informatique (virus, vers, chevaux de Troie, keyloggers, etc.) autrement appelé malware ;

- « consommable » : produit ou constituant qui disparait par l'usage des systèmes d'information et de communication (consommables d'impression, d'encre, etc.) ;

- « donnée à caractère personnel » : toute information relative à une personne physique identifiée ou identifiable (personne concernée), directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

- « filtrage » : ensemble des outils informatiques visant à limiter l'accès à certains sites Internet en raison de leurs contenus (contrôle des contenus, des URL, protocolaire, etc.) ;

- « matériel nomade » : moyens informatiques et de communication électronique portables et susceptibles en conséquence d'être utilisés à l'extérieur des locaux de l'entreprise ;

- « moyen d'authentification » : moyen permettant l'accès aux systèmes d'information et de communication et susceptible de prendre diverses formes : login/mot de passe, biométrie, signature électronique, cartes avec ou sans contact, etc. ;

- « scan sécurité » : ensemble d'outils informatiques qui permettent d'identifier, de contrôler et de protéger l'information grâce à des analyses de contenu approfondies, que l'information soit stockée, en mouvement ou traitée (un antivirus qui met en quarantaine les éléments infectés par des codes malveillants en recherchant les signatures virales dans les fichiers et les messages, un outil DLP ou « data loss prevention » qui prévient les fuites de données, etc.) ;

- « service en ligne » : service de communication par voie électronique de mise à disposition du public ou de catégories de public, de signes, de signaux, d'écrits, d'images, de sons ou de messages de toute nature qui n'ont pas le caractère de correspondance privée ;

- « systèmes d'information et de communication » : ressources et moyens informatiques et moyens de communication électronique appréhendés au sens large et recouvrant tout matériel informatique, câblage, périphériques (tels que imprimantes simples ou multifonctions, webcam, etc.), disque dur externe ou interne, carte mémoire, clé USB, ordinateur, tablette, photocopieurs, routeur, scanner, radiographie, etc., et toute ressource informatique de toute nature (logiciels, applications, bases de données, etc.), qu'ils soient accessibles à distance, directement ou en cascade à partir d'un réseau, ainsi les moyens de communication électronique recouvrant internet et les télécommunications (tels que téléphones, équipement sans fil, carte de communication sans fil, terminaux portables, tout

matériel nomade, messagerie, forum, sites web, etc.) et l'ensemble des données qu'il comporte ;

- « traces informatiques » : données informatiques témoignant de l'existence d'une opération au sein d'une application ou du système d'information.