CHARTE RELATIVE A LA SECURITE DES SYSTEMES D'INFORMATION

SOMMAIRE

1 Objet 3

2 Disposition Générale 3

3 Utilisation des Technologies Informatiques et de communication 4

4 Champ d'application 4

5 Principes généraux d'accès aux ressources informatiques 5

6 Dispositions relatives à l'utilisation des systèmes d'information et de communication 5

6.1 Usage des services Internet (Web, messagerie, forum…) 5

6.2 Messagerie 6

6.3 Usage du système d'information du groupe Umanis 7

7 Règles d'utilisation, de sécurité et de bon usage 8

8 Dispositions relatives à la sécurité des systèmes d'information et de communication 9

8.1 Conseils pour créer un mot de passe fort 11

9 Respect de la législation concernant les logiciels et le matériel 11

10 Dérogations 12

11 Dispositions relatives aux contrôles 12

11.1 Protection de l'intégrité et du bon fonctionnement des systèmes : Administration réseaux et sécurité 12

11.2 Analyse des malveillances avérées ou suspectées : Gestion des Incidents 13

12 Discipline et sanction 14

12.1 Rappel des principales lois françaises 15

1 OBJET

La présente charte informatique a pour objet de définir les règles d'utilisation des moyens informatiques mis à disposition par le Groupe Umanis.

L'utilisation de ces ressources doit être tournée vers la performance du Groupe Umanis et la satisfaction de ses clients internes et externes. Ces ressources font partie du patrimoine du Groupe Umanis.

Toutefois, l'utilisation relativement aisée de ces outils peut s'avérer potentiellement à très haut risque pour l'entreprise et ses collaborateurs.

Ainsi, chaque utilisateur doit être conscient que, d'une part, l'usage de ces ressources obéit à des règles qui s'inscrivent dans le respect de la loi et que, d'autre part, toute négligence ou mauvaise utilisation des ressources peut faire courir des risques à l'ensemble de l'entreprise.

L'**utilisateur** s'entend de toute personne, quel que soit son statut au sein du Groupe Umanis, c'est-à-dire salarié en contrat à durée indéterminée ou déterminée, stagiaire, contrats d'apprentissage, personnes détachées, personnel intérimaire ou intervenant extérieur utilisant les moyens informatiques de l'entreprise ainsi que ceux auxquels il est possible d'accéder à distance à partir du réseau administré par l'entreprise.

On entend par **système d'information** de l'entreprise : Le réseau administré par le Groupe Umanis, l'ensemble des matériels informatiques propriété du Groupe Umanis , connectés ou non au réseau administré par le Groupe Umanis (postes de travail fixes ou ordinateurs portables, serveurs, routeurs, photocopieurs, fax, téléphones fixes et portables, tablettes…), les logiciels, les moyens de communication du Groupe Umanis (messageries, accès Internet, etc.), ainsi que les informations et données propriété du Groupe Umanis (bases de données, documents, images, etc.).

2 DISPOSITION GENERALE

Les dispositions de la présente charte ont pour objet le rappel des bonnes règles de fonctionnement et d'utilisation du système d'information du Groupe Umanis afin de préserver la sécurité de celui-ci. Elles ne font pas obstacle à la loi dite Informatique et Libertés, aux articles de lois ou encore les jurisprudences existantes portant sur les droits de la personne et des salariés et sur les libertés individuelles, ni aux dispositifs prévus par le code du travail et des conventions collectives applicables tel le SYNTEC au-quel le Groupe Umanis est adhérant, ni encore à l'exercice du droit des institutions représentatives du personnel défini par les dispositions législatives, réglementaires ou statutaires.

La qualité d'utilisateur du Groupe Umanis implique la connaissance et le respect des règles exposées dans la présente charte relatives à l'utilisation des moyens informatiques. Le Groupe Umanis porte la présente charte à la connaissance de tout utilisateur de son système d'information.

3 UTILISATION DES TECHNOLOGIES INFORMATIQUES ET DE COMMUNICATION

Les technologies informatiques et de communication évoluent et offrent des opportunités réelles pour améliorer les performances de l'entreprise, à condition que les compétences informatiques des collaborateurs suivent ces évolutions et que leur utilisation s'inscrive dans le respect de règles générales et permanentes qui assurent la protection des systèmes d'information vis-à-vis des usages incorrects, abusifs ou malveillants qui peuvent avoir des conséquences désastreuses pour le Groupe, ses collaborateurs et ses clients.

Les règles de sécurité informatique en vigueur au sein du groupe sont définies, leur mise en place assurée et leur respect contrôlé par le service informatique du Groupe Umanis qui considère qu'assurer la sécurité de son système d'information et la tranquillité de ses utilisateurs sont des objectifs qui doivent être compris, assimilés et partagés par tous.

Ces objectifs ne peuvent être atteints que si les utilisateurs sont formés et qu'une relation de confiance est instaurée.

Ayant précisé le cadre légal de la présente charte, cette relation repose sur les principes suivants :

- **Transparence** : les règles fixent les interdits, précisent les limites d'une utilisation personnelle, décrivent la nature et les procédures de contrôles et les sanctions applicables exposées ci-après.
- **Sensibilisation :** Formation, Assistance : le Groupe Umanis met de nombreux moyens et ressources à la disposition des utilisateurs pour les sensibiliser à la sécurité, pour leur fournir une assistance technique renforcée, pour leur installer de nouveaux matériels et logiciels (Gestion de parc informatique) ou les aider lorsqu'ils sont victimes d'une malveillance (Gestion des incidents). En cas de besoin, les supérieurs hiérarchiques des utilisateurs sont tenus de leur préciser par écrit la marche à suivre en ce qui concerne les règles de sécurité informatique, l'utilisation du système d'information et du parc informatique du Groupe Umanis.
- **Responsabilisation** : Il est attendu de la part de chaque utilisateur, dans l'intérêt de tous, l'adoption au quotidien d'une attitude responsable et respectueuse des règles de conduite établies.

4 CHAMP D'APPLICATION

Les dispositions de la présente charte s'imposent à toute personne appelée **utilisateur** (cf.§ 1 Objet) amenée à :

- utiliser des « outils informatiques ou de communication » mis à sa disposition par le Groupe Umanis pour les besoins de son activité, tels que les équipements informatiques ou techniques (PC, serveurs, logiciels, badges d'entrée et de parking…) et les moyens de communication (téléphones fixes et mobiles, télécopies, messageries, accès intranet …),
- créer, consulter, mettre en œuvre, utiliser sous quelle que forme que ce soit les « ressources informatiques » de l'entreprise (informations, bases de données…),

5 PRINCIPES GENERAUX D'ACCES AUX RESSOURCES INFORMATIQUES

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder ne sont autorisés que dans **le cadre exclusif de l'activité professionnelle** des utilisateurs conformément à la législation en vigueur.

L'utilisation des ressources informatiques partagées de la société et la connexion d'un équipement sur le réseau sont en outre **soumises à autorisation**. Les autorisations sont demandées par le responsable hiérarchique de l'utilisateur. L'utilisateur est informé par le service informatique des autorisations accordées, leur date d'entrée en vigueur et de leur durée de validité. Ces autorisations sont **strictement personnelles** et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation même provisoire de l'activité professionnelle qui l'a justifiée.

- L'utilisateur est responsable de l'usage qu'il fait des ressources de l'entreprise en respect des règles de sécurité définies et mises en place par le Groupe. Cette utilisation doit être exclusivement professionnelle sauf exceptions expressément prévues au § 10 du présent document.
- Les outils mentionnés au paragraphe précédent ci-dessus font partie du patrimoine du Groupe Umanis, par conséquent, toute information donnée, reçue, émise ou stockée sur les équipements informatiques et les moyens de communication mis à disposition des collaborateurs demeure la propriété de l'entreprise sauf exceptions expressément admises au §10 du présent document (messages reçus et émis ayant un caractère personnel dûment identifiés comme tels).
- Les utilisateurs d'outils de communication qui leur sont mis à disposition, comme l'Internet, la messagerie électronique ou le téléphone véhiculent le nom et l'image du Groupe Umanis et doivent s'abstenir de toute action ou comportement pouvant y porter atteinte.
- Les utilisateurs doivent préserver le patrimoine et les intérêts du Groupe Umanis en respectant une obligation permanente de discrétion à l'égard de tout document interne et en particulier des informations considérées comme secrètes ou confidentielles en vertu de la procédure de protection des informations.
- La consultation de sites Internet à des fins personnelles est tolérée dans la mesure où elle n'entrave pas la réalisation des missions du collaborateur et qu'elle ne dégrade pas les performances du système.

6 DISPOSITIONS RELATIVES A L'UTILISATION DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

6.1 USAGE DES SERVICES INTERNET (WEB, MESSAGERIE, FORUM…)

Aucun utilisateur en aucune circonstance n'est autorisé à :

- Consulter, télécharger, stocker, publier, diffuser ou distribuer sous quelque support que ce soit, au moyen des ressources de l'entreprise, des documents, informations, images, audio, vidéos, etc. :
  - à caractère pornographique ou contraire aux bonnes mœurs,

- à caractère violent ou susceptibles de porter atteinte au respect de la personne humaine et de sa dignité, ainsi qu'à la protection des mineurs,
- à caractère diffamatoire et de manière générale illicite,
- portant atteinte aux ressources de l'entreprise et plus particulièrement à l'intégrité et à la conservation des données de l'entreprise,
- portant atteinte à l'image de marque de l'entreprise.

- Si l'utilisateur est amené à recevoir, à son insu, de tels éléments, il est tenu de les détruire aussitôt. Le Groupe Umanis recommande aux collaborateurs victimes de ces envois non désirés de contacter sans délai l'assistance de la Direction informatique (cf. §11.2 « Analyse des malveillances avérées ou suspectées : Gestion des Incidents »).
- En outre, l'utilisateur doit proscrire tout comportement pouvant inciter des tiers à lui adresser de tels documents sous forme d'informations, d'images, de vidéos, de fichiers, etc.
- Utiliser les ressources de l'entreprise à des fins de harcèlement, menace ou d'injure.
- Télécharger, stocker, utiliser, altérer ou transmettre des données, programmes, logiciels, progiciels, etc., qui sont protégés par les lois sur la propriété intellectuelle (ex : droits d'auteurs…), sauf à posséder les autorisations expresses nécessaires. L'utilisateur s'interdit de solliciter l'envoi par des tiers, en pièces jointes, de tels programmes, logiciels, progiciels, etc.
- Créer un site internet à titre personnel faisant référence au nom, au logo ou à toutes données de l'entreprise.
- Télécharger ou transmettre, sciemment, des fichiers contenant des virus, vers, chevaux de Troie, Rootkit, malwares … ou des données altérées.
- Répondre aux lettres en chaîne (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement. Ex : Chaîne d'amitié). Ce type de message a pour seul but de surcharger le réseau et d'affecter son bon fonctionnement, voire de véhiculer des éléments indésirables.
- Participer à un forum de discussion (« news group »), à des sites de dialogue en direct (« chat ») ou encore à des listes de diffusion (« mailing list ») sauf autorisation expresse dûment justifiée par l'exercice de fonctions particulières et/ou des raisons de service.
- Envoyer des messages en masse (plus de 20 destinataires, hors diffusion sur des listes de l'entreprise ou raison de service). En particulier, l'envoi de mails en mode « diffusion générale » est interdit aux collaborateurs et n'est réservé qu'aux seules personnes habilitées.
- Transférer, à l'extérieur de l'entreprise en dehors du contexte professionnel, des fichiers ou des documents, numérisés ou non, appartenant à l'entreprise sans l'accord de celle-ci. En cas d'accord, les transferts de fichiers ou documents doivent être effectués en appliquant les consignes de protection associées à leur classification.
- Communiquer son adresse électronique professionnelle sur des sites externes n'ayant pas de rapport avec son activité professionnelle.

6.2 MESSAGERIE

Le contenu des messages électroniques est confidentiel. Nul ne peut utiliser la messagerie d'un autre utilisateur sans l'autorisation expresse de ce dernier.

Tout message électronique émis ou reçu sur un poste Groupe Umanis est présumé professionnel sauf ceux ayant un caractère personnel et dûment identifiés comme tels ou adressés aux représentants du personnel et représentants syndicaux.

Le message électronique est un écrit pouvant engager UMANIS mais aussi son auteur. Il peut être reconnu comme preuve valable pour établir un fait ou un acte juridique. Chaque utilisateur doit donc porter une attention toute particulière à la rédaction d'un mail et à sa diffusion.

Le contenu d'un message ne doit pas porter atteinte aux intérêts et/ou à l'image de l'entreprise, de ses dirigeants ou de l'un de ses utilisateurs. En outre, l'utilisateur doit veiller à ne s'exprimer au nom de l'entreprise qu'après y avoir été autorisé, dès lors qu'il s'agit d'un message adressé à l'extérieur de l'entreprise (y compris lorsqu'un interlocuteur extérieur est en copie).

Aucun message électronique, y compris ceux relevant de l'utilisation privée (voir ci-après), ne devra comprendre des éléments de nature offensante, diffamatoire ou injurieuse.

Si un utilisateur est contraint d'adresser à l'extérieur des informations à caractère confidentiel ou nominatif, il devra demander l'assistance du service informatique pour que la confidentialité de ce mail soit garantie durant son transfert.

L'utilisation de la messagerie à des fins personnelles doit rester exceptionnelle, et l'utilisateur veillera à :

- Indiquer la mention « **privé** » ou « **personnel** » dans l'objet du mail,
- Classer ses mails privés (reçus ou envoyés) dans un répertoire ou dossier à part portant la mention «**privé**» ou «**personnel**» de manière à prévenir le service Informatique de la nature particulière des informations qu'il contient. Le service Informatique s'interdit la lecture de tels messages. Cette mention ne laisse cependant en aucun cas présumer du caractère non professionnel des mails. Ceux-ci peuvent donc être consultés par l'employeur après en avoir officiellement informé l'utilisateur et en présence de ce dernier,
- Ne pas faire figurer de texte ou de mention relative à l'entreprise et ne pas faire figurer d'indication qui pourrait laisser croire que le message est rédigé dans le cadre de l'exercice de ses fonctions.

L'ensemble des mails reçus et envoyés par les utilisateurs est conservé sur les serveurs du Groupe UMANIS. Les tailles des Boites à lettres sont limitées afin de préserver les performances du système de messagerie. Les mails doivent donc être archivés ou supprimés régulièrement par l'utilisateur. La fonction d'archivage permet de copier sur son poste de travail les mails que l'utilisateur désire conserver.

Chaque utilisateur doit organiser et mettre en œuvre les moyens nécessaires à la conservation des messages pouvant être indispensables ou utiles en tant qu'éléments de preuve.

6.3 USAGE DU SYSTEME D'INFORMATION DU GROUPE UMANIS

Le système d'information mis à la disposition des utilisateurs dans le cadre de la relation de travail est la propriété exclusive de l'entreprise. Il est protégé par un ou plusieurs mécanismes d'authentification mis en place par le Groupe, ce qui doit permettre d'éviter les utilisations

malveillantes ou abusives par un tiers. Cela n'a pas pour objet de transformer l'ordinateur de l'entreprise en un ordinateur à usage privé.

Par ailleurs, les usages suivants sont interdits :

- Télécharger et déposer des documents quel qu'ils soient sur un serveur de l'entreprise sans autorisation préalable des responsables habilités du service informatique,
- Utiliser les matériels informatiques et outils de communication sans respecter les règles techniques applicables et les prescriptions définies par l'entreprise.
- Se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités du service informatique,
- Utiliser les programmes, progiciels, logiciels, données mis à disposition par l'entreprise, en violation des lois sur la propriété intellectuelle, et notamment, reproduire, représenter, adapter, modifier, traduire, diffuser ces logiciels.
- Altérer, détériorer ou falsifier des données propriété du Groupe Umanis ou de tiers.
- Utiliser les ressources de l'entreprise de manière à gêner l'accès d'autres utilisateurs internes ou externes au Groupe Umanis (ex : déni de service),

7 REGLES D'UTILISATION, DE SECURITE ET DE BON USAGE

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale. L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins autres que professionnelles.

En particulier:

- il doit appliquer les recommandations de sécurité de la société tant au niveau de l'utilisation des moyens informatiques quel qu'ils soient, que des « bonnes pratiques » sécuritaires dans le cadre de ses activités professionnelles (assistance technique, forfait, prestation d'infra., production…),
- il doit assurer la protection de ses informations et il est responsable des droits qu'il donne aux autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition,
- il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater (Cf.§ 11.2),
- il doit solliciter le service informatique du Groupe Umanis et/ou suivre la procédure mise en place par ce dernier pour toute installation de logiciel,
- il choisit des mots de passe sûrs en conformité avec les règles de sécurité prescrites par le service informatique du Groupe Umanis, gardés secrets et en aucun cas ne doit les communiquer à des tiers,
- il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage,
- sans habilitation accordée, il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien ou de masquer sa véritable identité,

- il ne doit pas tenter de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre, directement ou indirectement. En particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification,
- il ne doit pas dégrader l'intégrité, la sécurité et le bon fonctionnement du bien commun que constitue le réseau informatique du Groupe Umanis. L'insertion d'équipements de communication ou d'applications au sein de l'infrastructure informatique de la société sont soumis à étude et autorisation du service informatique,
- il ne doit pas installer ou développer un programme ayant vocation à évaluer ou corrompre la sécurité des moyens informatiques internes et externes à la société,
- il ne doit pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles. Il doit appliquer la Politique du **bureau propre** (aucun dossier papier, confidentiel ou non, laissé en évidence) et de l'**écran vide** (aucune session informatique laissée active et accessible).

8 DISPOSITIONS RELATIVES A LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

Afin d'assurer efficacement la mise en œuvre d'une sécurité élémentaire de premier rang, de préserver la confidentialité du patrimoine du Groupe Umanis, et de prévenir toute action susceptible d'affecter l'intégrité ou le bon fonctionnement du système informatique, chaque utilisateur doit respecter strictement les dispositions suivantes :

- Le mot de passe permettant l'accès au poste de travail est strictement personnel et confidentiel. Il ne doit être communiqué à personne, même temporairement, afin d'éviter qu'une personne puisse usurper l'identité de l'utilisateur à son insu. Ce mot de passe doit être changé régulièrement (*à minima tous les mois*) et dans tous les cas dès qu'il est susceptible de ne plus être confidentiel. Il sera le reflet de la procédure de sécurité et plus particulièrement du paragraphe concernant la définition du mot de passe (§8.1 ci-dessous).
- Verrouiller son poste de travail en cas d'absence, même de courte durée (**ctrl+alt+suppr ou del, ou touche windows +L).**
- Les utilisateurs d'ordinateurs portables, doivent impérativement l'attacher avec son câble de sécurité à un support non amovible pendant la journée. Le soir ou le week-end, ils doivent l'enfermer obligatoirement dans une armoire ou un caisson, la clé restant en leur possession ou dans un lieu protégé. Si le portable contient des informations confidentielles, stratégiques pour le groupe, il doit être enfermé dans un coffre prévu à cet effet par le Groupe Umanis. La procédure de « *Gestion de prêt de matériel »* (sous la responsabilité du Service informatique), permet sur autorisation du supérieur hiérarchique de l'utilisateur, l'usage de l'actif hors des murs de l'entreprise, toujours en respect des termes de la présente charte.
- Les fichiers à caractère « confidentiel » stockés sur un ordinateur ou échangés par mail doivent être cryptés avec un logiciel de chiffrement (disponible auprès de la DSI), conformément aux règles de protection des informations classifiées. Le stockage, la destruction et l'échange de supports informatiques (clé USB, HDD portable, CD-ROM, …) contenant des données sensibles doivent respecter ces mêmes règles.

- Ne pas modifier la configuration de son poste de travail au niveau des périphériques, matériels et logiciels. De même ne pas modifier la configuration ou ne pas désactiver l'anti-virus (même en ce qui concerne les postes de développement).
- Si nécessaire et justifié, par un accord écrit du supérieur hiérarchique, faire une demande auprès du service informatique du groupe pour la modification provisoire de la configuration du poste de travail nécessaire à l'exercice de la mission.
- Ne pas essayer de désactiver la mise à jour de la base virale de l'anti-virus, ou d'empêcher voire interrompre les mises à jour du système d'exploitation du poste de travail.
- Détruire immédiatement et sans les ouvrir les messages dont la provenance est inconnue et dont les pièces jointes paraissent suspectes: ils peuvent contenir de dangereux virus, vers ou chevaux de Troie.
- Rester respectueux dans ses échanges en toutes circonstances. Chaque mail peut en effet être stocké et réutilisé à l'encontre de son auteur ou à l'encontre du Groupe Umanis par son destinataire et constituer un commencement de preuve par écrit.
- Ne pas oublier de récupérer, sur les fax, imprimantes ou photocopieurs, les documents sensibles que l'on envoie, imprime ou photocopie. Ils peuvent contenir des informations confidentielles pour l'entreprise et être de fait subtilisés par des tiers.
- En cas de malveillance interne ou externe constatée (ex : intrusion, vol), contacter le Responsable Sécurité du SI (**RSSI**).
- Badges électroniques :
  - chaque utilisateur travaillant sur les sièges du Groupe et détenteur d'un badge doit le porter en permanence sur lui et en est totalement responsable ;
  - Une gestion des prêts de badges, gérée par les Services Généraux, permet un suivi rigoureux des badges en circulation ;
  - aucun utilisateur ne peut prêter son badge personnel à quiconque dans des conditions non conformes aux prescriptions de l'entreprise ;
  - tout utilisateur travaillant sur les sièges du Groupe est tenu d'accompagner ses visiteurs dans les locaux. Les visiteurs doivent signer, à l'accueil, un registre d'entrée/sortie, précisant le nom de la personne visitée, les horaires d'arrivée et de départ, et doit présenter une carte d'identité pour laquelle il recevra un badge « Visiteur » qu'il devra porter de façon visible durant sa visite dans les locaux du groupe ;
  - aucun utilisateur en aucune circonstance n'est autorisé à utiliser son badge personnel dans des conditions frauduleuses ou non conformes aux prescriptions de l'entreprise.

L'entreprise se réserve la possibilité d'effectuer des vérifications et contrôles réguliers, dans les limites prévues par la loi.

L'absence de respect de ces prescriptions est susceptible de nuire à l'entreprise ou aux personnes qui s'y trouvent et pourra de ce fait être sanctionnée conformément aux dispositions du § 12 du présent document.

8.1 CONSEILS POUR CREER UN MOT DE PASSE FORT

Les mots de passe constituent la première ligne de défense contre tout accès non autorisé à votre ordinateur. Plus votre mot de passe est fort, plus votre ordinateur est protégé contre les pirates informatiques et les programmes malveillants.

Un mot de passe fort :

- comprend au moins huit caractères ;
- ne contient ni votre nom d'utilisateur, ni votre vrai nom, ni le nom de la société ;
- ne contient pas de mot entier ;
- est complètement différent des mots de passe précédents ;
- contient des caractères provenant de chacune des quatre catégories suivantes :

Catégorie de caractère	Exemple
Lettres majuscules	A, B, C…
Lettres minuscules	a, b, c…
Chiffres	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Symboles du clavier (tous les caractères du clavier non définis comme des lettres ou des chiffres) et espaces	` ~ ! @ # $ % ^ & * ( ) _ - + = { } [ ] \ | : ; " ' < > , . ? /

Un mot de passe peut répondre à tous les critères ci-dessus et rester faible malgré tout. Par exemple, « **Bonjour2U!** » ou « Passw0rd! » répondent à tous les critères de mot de passe fort mais reste faible car il contient un mot entier **« Bonjour 2 U!** » est un mot de passe plus fort parce que certaines lettres du mot entier ont été remplacées par des chiffres et parce qu'il contient également des espaces.

☞ *Si l'utilisateur ressent le besoin d'écrire son mot de passe pour le retenir, il convient de ne pas le nommez comme tel et surtout le conserver en lieu sûr.*

9 RESPECT DE LA LEGISLATION CONCERNANT LES LOGICIELS ET LE MATERIEL

Il est strictement interdit d'effectuer des copies de logiciels commerciaux pour quelque usage que ce soit, hormis une copie de sauvegarde dans les conditions prévues par le code de la propriété intellectuelle. Ces dernières ne peuvent être effectuées que par la personne habilitée à cette fin par le responsable. Par ailleurs l'utilisateur ne doit pas installer de logiciels à caractère ludique, ni contourner les restrictions d'utilisation d'un logiciel.

En outre l'utilisateur s'engage expressément à restituer :

- les matériels qui lui auront été confiés ainsi que toute copie ou reproduction de logiciels en sa possession,
- l'ensemble des fichiers ou bases de données informatiques, contenus dans son ou ses disques durs, qu'il aura crée ou modifié dans le cadre de ses fonctions au sein du Groupe Umanis, le jour même où il cessera effectivement ses fonctions (le jour de son départ effectif de l'entreprise), pour quelque cause que ce soit, sans qu'il soit besoin d'une demande ou d'une mise en demeure préalable par l'entreprise.

10 DEROGATIONS

Par dérogation l'utilisation à des fins extra-professionnelles des outils mis à disposition (téléphone, fax, internet messagerie, …) est exceptionnellement admise sous réserve de respecter les conditions suivantes :

- L'utilisation ne doit être que de courte durée, peu « volumineuse » et justifiée par les besoins ordinaires de la vie personnelle et familiale,
- Elle doit en conséquence s'inscrire dans le respect des règles exposées dans le présent document et ne pas mettre en péril la fiabilité et les performances du système d'information et du réseau, ni avoir pour effet de porter atteinte au patrimoine de l'entreprise, ses données sensibles ou sa notoriété, ou de porter préjudice aux personnes de l'entreprise ou hors de l'entreprise,
- Elle ne doit pas non plus détourner l'utilisateur de son activité dans des conditions mettant en jeu sa productivité ou en violation des dispositions énoncées dans le présent document.

11 DISPOSITIONS RELATIVES AUX CONTROLES

La nécessité de protéger l'entreprise et ses systèmes d'informations particulièrement lorsque des indices ou faits sérieux et concordants permettent d'identifier l'existence d'une utilisation illicite ou frauduleuse (ex : vol, vandalisme, intrusion, divulgation d'informations sensibles, déni de service, fraude …) contraire aux prescriptions du présent document, fonde les dispositions qui suivent dans le respect du principe de proportionnalité tel que visé à l'article L1121-1 du Code du Travail.

Ces dispositions visent également à rendre impossible ou à faire cesser toute infraction commise avec les moyens de l'entreprise, aux lois et règlements visant le respect de la personne humaine, la protection des mineurs, l'encouragement à la haine raciale, etc.

11.1 PROTECTION DE L'INTEGRITE ET DU BON FONCTIONNEMENT DES SYSTEMES : ADMINISTRATION RESEAUX ET SECURITE

Le bon fonctionnement des systèmes d'information et leur protection nécessitent une surveillance technique permanente automatisée afin de détecter et corriger les pannes, les virus, les attaques, les intentions malveillantes ou frauduleuses, les piratages, etc. Cette surveillance est assurée par l'Administration Réseaux (DSI) et le RSSI.

Ces services utilisent des outils automatiques permettant notamment :

- de détecter, a priori, à l'aide de systèmes à l'entrée ou à la sortie, tout type de fichier ou message non conforme ou dont la provenance permet d'identifier une source interdite ou illicite, dont la nature ou le contenu sort de l'ordinaire par la taille ou le type. Dans le cadre de leur fonction, les administrateurs peuvent ainsi être amenés à accéder aux messages électroniques à stricte fin de les débloquer ou éviter des démarches hostiles.
- d'analyser et de contrôler, a posteriori, les traces informatiques à fin d'études statistiques et de surveillance du réseau et des systèmes.
- Ces traces sont inhérentes aux systèmes et se matérialisent par des fichiers dits de « journalisation » qui permettent de conserver la mémoire des tâches accomplies, et notamment d'identifier pour chaque opération effectuée sur un système, son auteur, l'heure de sa réalisation, l'outil utilisé, les fichiers consultés ou encore d'établir la liste des sites les plus visités sur le Web.

11.2 ANALYSE DES MALVEILLANCES AVEREES OU SUSPECTEES : GESTION DES INCIDENTS

Afin de maîtriser l'évolution des incidents susceptibles de porter atteinte aux biens de l'entreprise ou des collaborateurs, le Groupe Umanis a mis en place un service de **Gestion des Incidents**, appelée « **GI** » ci-après (accessible par le biais de l'outil **SPOC** : **http://spoc.umanis.com**) chargé de l'analyse des causes des abus et des actes malveillants.

Un incident peut-être déclaré par tout collaborateur constatant une malveillance ou souhaitant prévenir une possible malveillance.

La GI procédera alors à une rapide analyse préliminaire pour vérifier son opportunité et décider s'il y a lieu, de traiter ou non la demande, en vertu du principe de proportionnalité et du cadre légal et réglementaire en vigueur. Si elle est valide, la requête sera alors adressée au DSI et au RSSI.

Sur requête d'intervention, les principales traces informatiques que la GI pourra consulter, sont notamment :

- Les outils ACD, SVI PABX …
- les listes d'appels des téléphones fixes sur PABX,
- les enregistrements vidéo,
- les journaux (traces informatiques) produits par les systèmes de badges,
- les journaux (traces informatiques) produits par les systèmes d'information eux-mêmes (applicatifs, bases de données…)
- les journaux (traces informatiques) produits par différents éléments du système d'information tels que notamment les systèmes d'exploitation, pare-feu, routeurs, relais internet, relais WIFI, messagerie, …

La durée de conservation des traces informatiques peut résulter d'obligations légales, mais dépend en premier lieu des fonctionnalités de chaque outil. Dans le Groupe Umanis, la durée de conservation des traces informatiques est généralement de six mois Les durées de conservation propres à chaque outil sont précisées par la procédure de gestion des incidents.

Par ailleurs, le contenu de tout message électronique dont l'objet ne mentionne pas le caractère personnel, comme il précisé au § 6.2 ci-dessus, pourra faire l'objet d'un contrôle dans le cadre d'une requête d'intervention.

12 DISCIPLINE ET SANCTION

Dans le respect du cadre législatif et réglementaire, l'entreprise peut en cas de survenance d'actes de malveillance ou illicites, d'atteinte à la sécurité de ses systèmes d'information ou de ses moyens de communication, supprimer, à titre conservatoire ou définitif, l'accès aux moyens de communication et utiliser les moyens appropriés pour préserver ses droits.

Le non-respect des règles ci-dessus énoncées engage la responsabilité personnelle de l'utilisateur dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables et l'expose à une sanction disciplinaire appropriée et proportionnée aux manquements commis dans les conditions de du règlement intérieur.

Il est à noter que les fautes légères sont aggravées par la récidive.

- Tout acte de nature à troubler le bon ordre et la discipline est interdit. A titre d'exemple et sans que cette énumération ait un caractère limitatif, sont considérés comme tels :
  - emporter du lieu de travail, sans autorisation, des objets, matériels et documents appartenant à la Société,
  - divulguer des secrets ou procédés de fabrication et manquer au secret professionnel ou à l'obligation de discrétion,
  - entraver le travail d'un ou plusieurs membres du personnel,
  - laisser volontairement ou par négligence se détériorer le matériel à sa disposition.
- Il est interdit à l'utilisateur :
  - d'utiliser des informations et/ou du matériel afin d'exercer une activité qualifiée de frauduleuse visant à détourner les Services du Groupe Umanis, pour son propre compte et/ou celui d'autrui,
  - d'utiliser des informations financières de manière illicite ; de manière générale, la diffusion de l'information financière est strictement réservée aux collaborateurs habilités,
  - d'utiliser ou de recopier illégalement et plus généralement de porter atteinte aux programmes et aux données informatiques protégées ou aux systèmes informatiques utilisés.
- En cas de faute ou d'infraction notamment aux prescriptions du présent document, aux notes de service prises en application, la Direction Générale se réserve le droit d'appliquer en considération de la gravité des fautes commises, l'une quelconque des sanctions suivantes conformément au Règlement Intérieur:
  - avertissement écrit,
  - mise à pied de 1 à 3 jours ou à titre exceptionnel pouvant aller jusqu'à 6 jours ouvrables,
  - licenciement,
  - poursuite judiciaire.

12.1 RAPPEL DES PRINCIPALES LOIS FRANÇAISES

Voici quelques extraits d'articles du code pénal concernant la sécurité informatique. Il est très important de prendre conscience que les interdictions et obligations existent et que les condamnations relatives sont très clairement définies.

CODE PÉNAL (Partie Législative)	Element Legal	Element Matériel
atteintes aux droits de la personne résultant des fichiers ou des traitements informatiques	**Art. 226-16**	Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en oeuvre prévues par la loi est puni de **cinq ans d'emprisonnement** et de **300 000 € d'amende**
	Art. 226-17	Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 de la loi nº 78-17 du 6 janvier 1978 précitée est puni de **cinq ans d'emprisonnement** et de **300 000 Euros d'amende**.
	Art. 226-18	Le fait de collecter des données à caractère personnel par un moyen frauduleux, déloyal ou illicite est puni de **cinq ans d'emprisonnement** et de **300 000 € d'amende**.
	Art. 226-21	Le fait, par toute personne détentrice de données à caractère personnel à l'occasion de leur enregistrement, de leur classement, de leur transmission ou de toute autre forme de traitement, de détourner ces informations de leur finalité telle que définie par la disposition législative, l'acte réglementaire ou la décision de la Commission nationale de l'informatique et des libertés autorisant le traitement automatisé, ou par les déclarations préalables à la mise en oeuvre de ce traitement, est puni de **cinq ans d'emprisonnement** et de **300 000 € d'amende.**
	Art. 226-22	Le fait, par toute personne qui **a recueilli**, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir est puni de **cinq ans d'emprisonnement** et de **300 000 € d'amende**. La **divulgation** prévue à l'alinéa précédent est punie de **trois ans d'emprisonnement** et de **100 000 € d'amende** lorsqu'elle a été commise par imprudence ou négligence.
	Art. 323-1	Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement** et de **30000 euros d'amende**. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende. Ces systèmes comprennent, entre autre, les sites web
	Art. 323-2	Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de **cinq ans d'emprisonnement** et de **75000 euros d'amende**.
	Art. 323-3	Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de **cinq ans d'emprisonnement** et de **75000 euros d'amende**.