CHARTE D'UTILISATION DU SYSTEME D'INFORMATION

GROUPE SEGULA TECHNOLOGIES

Préambule

Le Groupe SEGULA Technologies met à la disposition de tout utilisateur des Equipements Informatiques et des Moyens de Communication, ainsi que des Informations et des Données qui sont nécessaires à l'accomplissement de ses fonctions et de ses missions.

Chaque Utilisateur est informé que l'usage des Ressources Informatiques et du Système d'Information obéit à des règles qui s'inscrivent dans le respect de la loi, de la sécurité et du bon usage, gages d'efficacité opérationnelle, et doit être conscient que sa négligence ou sa mauvaise utilisation fait courir des risques au Groupe, et donc à lui-même.

Dans un but de transparence à l'égard des Utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du Système d'Information, la présente charte pose les règles relatives à l'utilisation de ces ressources (ci-après la « Charte »).

La Charte ne fait pas obstacle à ce que des dispositions spécifiques soient définies par le Groupe en vue d'une utilisation du Système d'Information par les représentants du personnel.

1. STATUT DE LA CHARTE

1.1 OBJET DE LA CHARTE

L'objet de la présente Charte est de préciser la responsabilité des Utilisateurs et de les informer de leurs devoirs ainsi que de leurs droits concernant l'utilisation des Ressources Informatiques et du Système d'Information.

Elle garantit et encadre le respect du droit à la vie privée pour les Utilisateurs.

1.2 CHAMP D'APPLICATION

La Charte s'adresse à l'ensemble des Utilisateurs ayant recours au Système d'Information, quels que soient leurs statuts et leurs fonctions.

Elle est présentée pour information au Comité d'Entreprise, elle est portée à la connaissance de l'ensemble du personnel du Groupe par affichage sur les panneaux prévus à cet effet, elle est mise à disposition sur l'intranet du Groupe.

Un exemplaire de la présente Charte est remis contre récépissé à tout nouveau collaborateur au moment de son entrée en fonction. La signature de ce récépissé engage le collaborateur au respect de ladite Charte. La DSI lui délivre alors ses codes d'accès au Système d'Information. A défaut de ce récépissé signé, la DSI ne délivre pas de codes d'accès.

Il en est de même pour tout Utilisateur Tiers, c'est-à-dire n'étant pas salarié du Groupe et ayant accès au Système d'Information.

De même, tous les salariés du Groupe travaillant en clientèle ou sur un plateau Client s'engagent à respecter les dispositions de la Charte Informatique du Client.

2. MODALITES D'APPLICATION DE LA CHARTE

2.1.1 Exécution de la Charte

La Direction des Systèmes d'Information du Groupe (ci-après la « DSI ») met en place et est chargée de toutes les mesures techniques nécessaires à son application et au contrôle de son respect.

La DSI dispose de droits spécifiques (dits « administrateur »). Elle est également chargée de la surveillance du trafic sur les réseaux du Groupe.

2.1.2 Non-respect et sanctions

Le non-respect des règles et mesures de sécurité figurant dans la présente Charte engage la responsabilité personnelle de l'Utilisateur ou de l'Utilisateur Tiers dès lors qu'il est prouvé que les faits fautifs lui sont personnellement imputables (ou ont été commis au moyen de codes d'accès dont il est responsable) et peuvent faire l'objet de poursuites pénales.

Par ailleurs, toute infraction aux dispositions de la présente Charte est susceptible de justifier la suspension immédiate de l'utilisation du Système d'Information et/ou le cas échéant le lancement de procédures disciplinaires prévues par les textes en vigueur, réserve étant faite de tous autres droits et actions à l'encontre de l'Utilisateur que peuvent engager les tiers ou le Groupe lui-même.

3. DEFINITIONS

Les termes commençant par une lettre majuscule, utilisés ci-avant ou ci-après dans la présente Charte, sont définis comme suit :

« Equipements Informatiques » : désignent l'ensemble des outils utilisés par l'Utilisateur dans le cadre de sa mission (PC, stations, imprimantes, logiciels, tablettes numériques, téléphones portables, smartphones, supports amovibles tels disques durs externes, clés USB etc.…) mis à sa disposition par le Groupe.

« Moyens de Communication » : désigne l'ensemble composé de la messagerie électronique individuelle du Groupe, l'internet, l'intranet, les espaces de communication publics ou Groupe (type blogs, Facebook…).

« Données » : désignent globalement l'ensemble des informations qui transitent ou qui sont stockées sur le Système d'Information, et dont l'Utilisateur a connaissance dans l'exercice de sa fonction. Elles relèvent généralement de l'obligation de discrétion professionnelle.

« Données Sensibles » : désignent l'ensemble des informations pouvant faire l'objet de restrictions d'accès ou d'usage. Une infraction aux restrictions d'accès à ces données peut relever du Code pénal. Elles peuvent faire l'objet d'un marquage d'identification particulier. Elles concernent notamment :

- La protection SECRET DE DEFENSE
- Protection du patrimoine NATIONAL
- Protection du patrimoine PRIVE
- Protection de la VIE PRIVEE

Le cas échéant, le Groupe, la DSI ou le Responsable Sécurité pourront classer explicitement un ensemble de données comme étant des « Données Sensibles ». Dans ce cas, les Utilisateurs concernés seront dûment informés de cette classification, de telle sorte qu'il ne pourra subsister aucun doute pour eux quant à cette classification.

« Groupe» : désigne l'ensemble des entités contrôlées effectivement, directement ou indirectement par SEGULA Technologies.

« Ressources Informatiques » : désignent les Equipements Informatiques et les Moyens de Communication ; les Ressources Informatiques font partie intégrante du Système d'Information du Groupe.

« Système d'Information » : désigne l'ensemble des composants applicatifs, des plateformes, des infrastructures matériels et réseaux, et tout dispositif de sécurité, dont les Ressources Informatiques, administré et géré directement ou indirectement par la DSI du Groupe et participant à la gestion, au stockage, au traitement, au transport et à la diffusion des Données.

« Utilisateur » : toute personne, membre du personnel du Groupe, à titre permanent ou temporaire, ou toute personne exerçant son activité dans les locaux du Groupe, quel que soit son statut, notamment le personnel intérimaire, les stagiaires, les consultants, les partenaires, utilisant le Système d'Information.

4. REGLES D'UTILISATION DU SYSTEME D'INFORMATION

4.1 UN USAGE RESPONSABLE

L'Utilisateur contribue à la sécurité générale du Système d'Information du Groupe en appliquant les recommandations de sécurité.

Il s'engage à ne pas perturber le bon fonctionnement de ce Système par son action ou son inaction et à ne pas dégrader les Ressources Informatiques.

Il s'engage à ne pas désactiver ou contourner les mesures ou dispositifs de sécurité. Il s'assure à son niveau du bon fonctionnement de ces dispositifs de sécurité, notamment de celui relatif à l'antivirus.

L'usage des Ressources Informatiques du Groupe est réservé au cadre professionnel.

Chaque Utilisateur veille à un emploi mesuré et raisonné des Ressources Informatiques afin de permettre une bonne qualité de service au plus grand nombre.

Les Ressources Informatiques sont la propriété du Groupe. Les Données stockées sur le Système d'Information (à l'exception de celles concernant exclusivement la vie privée de l'Utilisateur) sont la propriété du Groupe ou de ses Clients.

Les logiciels sont, soit la propriété du Groupe, soit des logiciels utilisés par le Groupe dans le cadre d'une licence.

Chaque Utilisateur est responsable de l'accès et de l'utilisation des Ressources Informatiques mises à sa disposition et à ce titre doit respecter les règles générales d'éthique, de secret professionnel, de déontologie ainsi que d'un devoir de réserve, de discrétion et de loyauté envers le Groupe.

En aucune circonstance et sous aucun prétexte, l'Utilisateur ne pourra charger, stocker, publier, diffuser ou distribuer, des documents, informations, images et quelques autres données que ce soit :

- à caractère violent, pornographique ou contraire aux bonnes mœurs, et/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 Informatiques et au Système d'Information du Groupe et plus particulièrement à l'intégrité et à la conservation des données du Groupe.

4.2 UTILISATION DES RESSOURCES INFORMATIQUES

4.2.1 Accès aux Ressources Informatiques

La DSI met en place un accès nominatif pour réguler l'accès aux Données.

Le contrôle d'accès au Système d'Information permet d'identifier toute personne utilisant les Ressources Informatiques et le Système d'information, et notamment les messageries électroniques. Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque Utilisateur sur les Ressources Informatiques du Système d'Information dont il a besoin pour son activité.

Une identification est confiée à chaque Utilisateur. Le plus souvent, elle est matérialisée par un login (identifiant) et un mot de passe.

Les droits d'accès peuvent être retirés à tout moment et prennent fin lors de la cessation de l'activité professionnelle.

L'Utilisateur s'engage à respecter les procédures administratives relatives à l'attribution de droits d'accès en vigueur dans le Groupe. Ces procédures s'appliquent en particulier lors de la prise de fonction, d'une mutation ou d'un départ.

L'Utilisateur ne doit pas masquer son identité ou tenter d'usurper celle d'un autre.

D'une manière générale, il ne doit pas accéder à ou utiliser des Ressources Informatiques autres que celles auxquelles il a légitimement accès. Il lui est interdit de tenter de lire, modifier, copier ou détruire des Données ou documents autres que ceux dont il a légitimement l'usage.

L'Utilisateur s'assure, avant de s'absenter de son bureau, qu'il s'est déconnecté des Ressources Informatiques en cours d'utilisation.

Toute tentative d'intrusion constatée doit être signalée sans délai au responsable hiérarchique de l'Utilisateur et à la DSI.

4.2.2 Confidentialité des codes d'accès

Les codes d'accès sont personnels et confidentiels. Ils ne doivent en aucun cas être communiqués par leur titulaire à un tiers, que ce dernier soit membre du personnel du Groupe ou non.

L'Utilisateur s'engage, sous son entière responsabilité, à maintenir ses codes d'accès secrets : la divulgation volontaire ou par négligence de codes d'accès est considérée comme une faute professionnelle et, par conséquent, elle est passible de sanctions. Il est précisé que l'Utilisateur pourra toutefois communiquer ses codes d'accès à son responsable hiérarchique à la demande motivée et écrite de ce dernier. Dans ce cas, l'utilisateur veillera à changer ses codes dès que la situation sera revenue à la normale.

Chaque utilisateur dispose principalement de deux mots de passe. Le premier mot de passe concerne les systèmes Windows, l'ouverture de session Windows, l'accès aux serveurs de fichiers, la messagerie et tout autre système connecté à l'Annuaire Windows appelé « Active Directory » ou AD. Ce mot de passe doit être changé régulièrement, au minimum tous les 3 mois. La DSI s'efforce de connecter l'ensemble des applications à l'Active Directory pour quelle bénéficient de l'authentification par l'Active Directory.

Le second mot de passe donne accès aux applications ne bénéficiant pas encore de l'authentification par l'Active Directory. Ce mot de passe est attribué par la DSI dans l'application « AIGLE » et n'est pas modifiable par l'utilisateur.

Certaines applications particulières disposent de leurs propres mots de passe, qui sont alors soumis à des règles de changement propres à chacune de ces applications.

Les codes d'accès doivent être de préférence mémorisés par l'Utilisateur. Dans le cas où la conservation du code d'accès sous forme lisible s'avérerait nécessaire, ce dernier doit être stocké par l'Utilisateur, sous sa responsabilité, dans un endroit secret et sous-clé afin de ne pas être accessible à autrui. En tout état de cause, la compromission éventuelle des codes d'accès doit être facilement et rapidement détectable par l'Utilisateur.

Une fois divulgués ou après la découverte de leur compromission, les codes d'accès doivent être immédiatement changés par l'Utilisateur ou la DSI selon le cas.

De manière générale, toute utilisation des Ressources Informatiques au moyen des codes d'accès d'un Utilisateur engagera la responsabilité de ce dernier.

L'Utilisateur ne doit pas modifier la configuration des Ressources Informatiques mis à sa disposition par le Groupe en installant ou en désinstallant des périphériques, des logiciels, des progiciels, (y compris les programmes libres de droit). Seule la DSI du Groupe est habilitée à réaliser ces opérations.

En particulier, l'Utilisateur ne dispose pas des autorisations et des privilèges pour prendre le contrôle total des Ressources Informatiques lui étant confiées. L'utilisation des comptes de type « administrateur » est interdite, sauf habilitation par la DSI matérialisée par un document signé entre la DSI et l'Utilisateur.

4.2.3 Sécurité

Les déplacements des Equipements Informatiques fixes sur les sites du Groupe sont assujettis à une procédure de déménagement, contrôlée par la DSI du Groupe.

Chaque Utilisateur est tenu d'informer la DSI:

- du vol ou de la dégradation de son Equipement Informatique,
- du dysfonctionnement éventuel de l'Equipement Informatique qu'il utilise,
- du changement d'Utilisateur de l'Equipement Informatique dont il est responsable.

Les informations contenues dans un Equipement Informatique sont facilement exploitables s'il est volé ou perdu. Le mot de passe ne constitue pas un obstacle suffisant et des protections supplémentaires doivent être mises en œuvre.

Voici donc quelques règles simples à suivre obligatoirement :

1 – En quittant son bureau, quelle que soit la durée de son absence, l'Utilisateur doit verrouiller sa session (ex. : Ctrl + Alt + Suppr, puis « Verrouiller »)

2 – En l'absence de l'Utilisateur, tout ordinateur fixe ou portable doit être sécurisé de l'une des façons suivantes :

- il sera attaché à un bureau par un câble antivol. Cela concerne les portables comme les PC de bureau ;
- il sera mis sous clef dans une armoire fermant à clef (et bien sûr la clef ne se trouvera pas sur l'armoire !)

- le bureau sera lui-même fermé à clef.

3 – Lors d'un déplacement, les ordinateurs portables doivent être sécurisés par un câble antivol, partout, que ce soit dans un lieu public (train), un site du Groupe ou un site d'un client du Groupe. La DSI vous fournira un câble adapté sur simple demande.

D'une manière générale, les Utilisateurs de supports électroniques portables (et notamment, sans que cette liste soit limitative, ordinateur portable, tablette numérique, smartphone) ne doivent jamais les laisser sans surveillance.

4.2.4 Utilisation de supports amovibles

L'Utilisation des applications communicantes (internet, messagerie, etc.) et des supports de stockage amovibles (disquette, CD-Rom, clef USB), peut, malgré les précautions prises, provoquer la transmission et l'installation sur le poste de travail de l'Utilisateur, de programmes ou fichiers, qui altèrent ou pillent les Données et logiciels qu'il contient.

L'utilisation de supports de stockage amovibles doit donc être limitée aux supports dont l'origine est connue. Il est interdit d'utiliser des supports de stockage amovibles d'origine douteuse, sans y avoir été autorisé par la DSI. A titre d'exemple, une clef USB trouvée dans un couloir ou un parking, ou remise par une personne inconnue, ne doit pas être branchée sur son poste de travail ou sur son ordinateur portable sans être passée par la DSI.

Sur certains Equipement Informatiques, l'utilisation de supports de stockage peut être strictement interdite ou soumise à des conditions d'utilisation spécifiques. L'Utilisateur devra se soumettre aux prescriptions particulières attachées à ces Equipements Informatiques. Il s'agit notamment des Equipements Informatiques traitant des Données Sensibles (§ 3).

4.2.5 Lutte antivirale

La possession, l'utilisation ou le développement délibérés de programmes mettant en cause l'intégrité du Système d'Information sont interdits. L'introduction, volontaire ou non d'un virus est une mise en cause de l'intégrité du Système.

L'Utilisateur doit respecter toutes les mesures visant à empêcher l'introduction ou la diffusion de virus dans le Système d'Information. En cas de tentative d'intrusion ou d'intrusion constatée d'un virus dans le Système d'Information, l'Utilisateur doit en alerter exclusivement la DSI.

La DSI, responsable de la sécurité des réseaux, est seule habilitée à diffuser toute information sur les virus informatiques.

5. LA PROTECTION DES DONNEES

5.1 CONFIDENTIALITE

L'Utilisateur est tenu de respecter la confidentialité des Données auxquelles il a accès ou qu'il gère, conformément aux obligations de secret professionnel et de discrétion à sa charge.

Cette règle s'applique tant pour le traitement des Données que pour leur communication interne et externe.

Il s'engage à appliquer aux Données numériques les standards de gestion et de diffusion applicables aux informations et aux documents papiers conformément à leur niveau de sensibilité (donnée non protégée, donnée à diffusion restreinte, donnée confidentielle, etc) et à adopter le niveau de

protection adéquat. La transmission de Données Sensibles (§ 3) peut être autorisée selon les procédures particulières validées par le Responsable Sécurité et entre utilisateurs disposant d'un dispositif de chiffrement agréé par la DSI.

Il est notamment interdit à un Utilisateur, sauf autorisation ou demande préalables du Groupe, de communiquer des informations confidentielles du Groupe, que ce soit en interne, vers un tiers ou à destination de ses propres messageries personnelles.

5.2 L'ESPACE DE STOCKAGE DE L'UTILISATEUR

Tout Utilisateur pourra se voir attribuer un espace de stockage de données pour effectuer son travail, soit sur le serveur, soit en local sur les postes de travail. Les Données qu'il traite peuvent être partagées après en avoir fait la demande à la DSI.

L'espace de stockage mis à la disposition de l'Utilisateur est réservé aux fichiers professionnels de l'Utilisateur et demeure la propriété du Groupe. Il ne peut contenir que subsidiairement des informations relevant de l'intimité de la vie privée de l'Utilisateur. L'espace de stockage correspondant doit être libellé de façon claire et non ambigüe mentionnant le terme « Personnel », l'Utilisateur s'interdisant d'enregistrer, de stocker et/ou archiver des Données sur son espace de stockage personnel.

Un usage raisonnable, notamment en nombre et en volume, est donc toléré dans le cadre des nécessités de la vie courante et privée, à condition que l'utilisation des fichiers n'affecte ni l'espace de stockage, ni ne perturbe l'activité professionnelle de l'Utilisateur.

Un quota concernant la limite de stockage pourra être mis en place. L'Utilisateur effacera ses fichiers obsolètes, locaux ou bien en réseau, pour ne pas encombrer les Ressources Informatiques du Système d'Information.

L'Utilisateur est responsable de la licéité des fichiers stockés. Les fichiers stockés dans cet espace de stockage doivent l'être dans le respect de la présente Charte.

Il est strictement interdit d'y déposer des fichiers (logiciels, modules…) exécutables de manière explicite ou masquée qui n'auraient pas été autorisé et/ou fourni par la DSI.

De même, aucun fichier ne doit comprendre des éléments de nature offensante, diffamatoire, injurieuse, dénigrants tant à l'égard des autres Utilisateurs que du Groupe et de tout tiers extérieur au Groupe.

5.3 LA SAUVEGARDE DES DONNEES

La responsabilité de la sauvegarde des Données stockées sur les serveurs incombe au service d'exploitation de la DSI.

Aucune sauvegarde n'est faite sur les Equipements Informatiques en local (fixes ou portables).

Il appartient à chaque Utilisateur de sauvegarder les Données stockées sur le disque dur de son poste de travail en utilisant régulièrement les différents moyens mis à sa disposition (serveurs de fichiers, demande de création de CD-Rom ……).

La sauvegarde des Données Sensibles est en principe interdite et en tout état de cause cette sauvegarde est soumise à des règles et des systèmes spécifiques fixées par le Responsable Sécurité, mises en œuvre par la DSI et communiquées aux salariés concernés. Ces dispositions particulières sont conformes aux différentes règlementations applicables ou exigences clients en vigueur.

La sauvegarde des fichiers personnels est sous la responsabilité de l'Utilisateur.

5.4 DONNEES SENSIBLES

Certains Utilisateurs travaillent, dans le cadre de leur mission, sur des Données Sensibles. La transmission des Données Sensibles est interdite sauf dispositif validé par le Responsable Sécurité du Groupe, mis en œuvre par la DSI et porté à la connaissance des Utilisateurs concernés. Ces Données relèvent des articles 413-9 et suivants du Code pénal et que l'absence de respect des dispositions prévues pour leur protection peut avoir pour conséquence de mettre en jeu la responsabilité pénale des Utilisateurs.

Les Utilisateurs disposant de Données Sensibles doivent prendre toutes les mesures requises à des fins de protection de ces données et utiliser les systèmes de sécurité validé par le Responsable Sécurité du Groupe, mis en œuvre par la DSI et portés à leur connaissance,

5.5 DONNEES SENSIBLES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés (dite « Informatique et Libertés »), définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978.

Enfin, les traitements de données à caractère personnel (donc toutes les données nominatives) doivent être déclarés à la Commission Nationale de l'Informatique et des Libertés (CNIL), en vertu de la loi Informatique et Libertés. Les Utilisateurs souhaitant réaliser des traitements relevant de ladite loi sont invités à prendre contact avec la DSI avant d'y procéder.

6. REGLES D'UTILISATION DE LA MESSAGERIE

6.1 PRESENTATION ET REGLES GENERALES

6.1.1 Messagerie électronique individuelle

Chaque Utilisateur possédant une messagerie électronique individuelle mise à sa disposition par le Groupe dispose également d'une adresse e-mail qui le relie au réseau mondial Internet. Il est ainsi en mesure d'échanger des informations (envoi et réception) avec des personnes extérieures au Groupe.

L'adresse e-mail de chaque compte de messagerie électronique individuelle est généralement structurée de la manière suivante : prénom.nom@segula.fr.

6.1.2 Messagerie électronique privée

Certains fournisseurs d'accès proposent une adresse email avec la possibilité de consulter la messagerie électronique individuelle via un site Internet, sans qu'il soit nécessaire de disposer d'un logiciel de messagerie. Ce type de service est appelé WEBMAIL. L'utilisation de services WEBMAIL hébergés, de type Hotmail, pour la consultation de sa messagerie personnelle, est tolérée dans la mesure où cela n'interfère pas avec l'activité professionnelle de l'Utilisateur et où l'Utilisateur respecte les règles décrites au § 7.

6.1.3 Outil professionnel, usage personnel

La messagerie électronique du Groupe est un outil de travail à part entière. L'Utilisateur est tenu de la consulter les jours travaillés au minimum une (1) fois par jour, hormis en période d'absence. L'Utilisateur doit accorder la même importance aux messages électroniques reçus sur cette messagerie qu'aux courriers postaux ou fax et se doit de les traiter dans les meilleurs délais.

L'Utilisateur doit faire preuve de la plus grande correction et courtoisie à l'égard de ses interlocuteurs dans les échanges effectués par l'intermédiaire de la messagerie électronique du Groupe.

Par ailleurs, l'Utilisateur doit rédiger des messages courts et clairs afin d'éviter toute surcharge informationnelle nuisant à l'efficacité de la communication. Il doit également limiter le nombre de personnes mises en copie d'un message électronique, et éviter de « Répondre à tous » si cela n'est pas justifié.

Bien que la messagerie électronique du Groupe soit un outil de communication professionnelle, un usage personnel raisonnable, notamment en nombre et en volume, est toléré dans le cadre des nécessités de la vie courante et privée, à condition que l'utilisation de la messagerie électronique soit conforme aux dispositions de la présente Charte, ainsi qu'aux dispositions légales en vigueur, et qu'elle n'affecte ni le trafic normal des messages professionnels ni ne perturbe l'activité professionnelle de l'Utilisateur.

Les messages personnels ne doivent contenir aucune signature automatique au nom du Groupe.

L'usage de la messagerie électronique du Groupe pour la diffusion de messages (i) illicites, (ii) à caractère politique, (iii) religieux, (iv) ou d'informations de toute nature portant sur l'activité syndicale des salariés du Groupe est interdite, quel que soit le nombre de destinataires de ces messages.

Tout message reçu ou envoyé depuis la messagerie électronique individuelle mise à disposition par le Groupe, est considéré comme revêtant un caractère professionnel, sauf indication expresse dans l'objet du message de son caractère « Personnel ».

Il est formellement interdit de falsifier la source d'éléments contenus dans un fichier.

En cas d'absence prolongée d'un Utilisateur, il peut être demandé à la DSI de créer un message d'absence et une règle de transfert des messages vers la boîte aux lettres d'autres Utilisateurs, ce afin de permettre une continuité dans le fonctionnement du Groupe.

En cas de départ du Groupe, la boîte aux lettres de l'Utilisateur est close à sa date de départ par la DSI sur demande de la DRH. Elle sera ensuite supprimée dans un délai d'un mois.

6.2 MESSAGES EN MASSE

La diffusion massive de messages est susceptible de perturber le bon fonctionnement du réseau. L'Utilisateur n'est donc pas autorisé à envoyer des messages en masse, en chaîne ou de pétition (messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à le renvoyer également collectivement).

L'Utilisateur doit éviter l'envoi de copies à un nombre injustifié de destinataires et limiter au strict nécessaire les envois groupés à plusieurs personnes. Les messages doivent être envoyés aux seuls destinataires intéressés et concernés par le sujet. Par défaut, le nombre maximum est de 12 destinataires par mail, et la taille maximum des pièces jointes est de 5 Mo.

Les destinataires qui utilisent, pour répondre à un message illicite, la fonction « répondre à tous » sont aussi fautifs que l'émetteur initial, et sont, à ce titre, passibles de sanctions.

6.3 MESSAGERIE ELECTRONIQUE DU GROUPE ET INTERNET

6.3.1 Internet, un espace ouvert et perméable

Internet est un réseau ouvert et peu sécurisé, où la confidentialité des messages n'existe pas. Un acte de piratage y est toujours possible.

Internet ne permet pas d'identification fiable de l'expéditeur d'un message, ni de vérification du nom du destinataire. La prudence s'impose.

6.3.2 Lutte anti-spamming

On entend par « spam », l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière.

L'Utilisateur s'engage à ne pas répondre aux spams reçus, et à ne pas cliquer sur les liens hypertextes insérés dans le corps des spams. Ces actions permettent au « spammeur » d'établir que l'adresse mail est valide et qu'il peut continuer à le « spammer » ou revendre son fichier ou ses fichiers à d'autres « spammeurs ».

Lorsqu'il envoie un message simultané à plusieurs personnes, dont des personnes externes au Groupe, l'Utilisateur doit veiller à ne divulguer les adresses d'autres Utilisateurs que s'il apparaît nécessaire que leur identité et adresse soient connues de l'ensemble des destinataires. Cette divulgation sera faite à bon escient.

L'Utilisateur s'engage à ne pas communiquer à des tiers des adresses mail autres que la sienne sans le consentement préalable des intéressés.

6.3.3 Le danger des virus

Les virus sont généralement contenus dans les pièces jointes aux messages. Il convient de se méfier des messages d'origine douteuse. L'Utilisateur doit donc faire preuve de vigilance notamment vis à vis des messages envoyés par des auteurs inconnus, souvent rédigés en anglais, et comportant une pièce jointe. La conduite à suivre :

- ne pas ouvrir la pièce jointe et particulièrement les fichiers exécutables avec extension « .exe » ou «.vbs» ;
- ne pas transmettre le message à d'autres personnes (pour éviter les phénomènes de panique qui ne feraient qu'accroître le risque et saturer la messagerie) ;
- détruire le message ;
- s'il y a le moindre doute, contacter la DSI.

6.4 RESPONSABILITE PROFESSIONNELLE ET JURIDIQUE

L'Utilisateur de la messagerie électronique du Groupe est responsable vis-à-vis du Groupe quant à son utilisation. Le contenu des messages qu'il envoie, que ce soit le corps du message ou les pièces jointes, doit être conforme à la législation en vigueur en matière de droits d'auteur, de diffusion d'informations et d'expression d'opinions à caractère violent, pédophile, discriminatoire ou raciste (ou incitatives de tels comportements), de respect de la vie privée, etc.

6.4.1 L'Utilisateur est responsable du contenu des messages

Un message électronique peut constituer une preuve ou un commencement de preuve par écrit susceptible d'engager la responsabilité du Groupe. Il est fait interdiction à l'Utilisateur d'émettre une quelconque opinion personnelle, étrangère à son activité professionnelle et susceptible, par son caractère illicite, de porter préjudice au Groupe.

Tout courrier électronique engageant le Groupe doit respecter les règles formelles de validation éventuellement en vigueur au sein de chaque direction.

6.4.2 La responsabilité des boîtes aux lettres

Chaque Utilisateur est responsable de l'utilisation de sa boîte aux lettres, même en cas d'utilisation de celle-ci par un tiers, ce qui constitue une raison supplémentaire pour respecter les règles de sécurité des codes d'accès.

6.4.3 Délégation de boîtes aux lettres

L'Utilisateur qui a délégué la gestion de sa boîte aux lettres à un tiers assume la responsabilité des messages qui circulent via cette boîte.

6.4.4 Messages et documents à détruire

La Loi interdit le stockage et la diffusion de messages ou documents de nature diffamatoire, discriminatoire, pédophile ou incitant à la violence ou à la haine raciale.

Par conséquent, si un Utilisateur reçoit des messages ou des documents de cette nature il doit :

- alerter la DSI qui engagera les actions nécessaires,
- effacer ces documents de sa messagerie ou de son Equipement Informatique.

Le stockage, sur un équipement du Groupe, de documents de cette nature constitue une faute grave passible de sanctions.

6.4.5 Confidentialité

La messagerie électronique du Groupe est un espace confidentiel. Tout Utilisateur est tenu à une obligation générale et permanente de confidentialité et de discrétion à l'égard des informations et documents électroniques disponibles sur le réseau interne. Ceci implique de s'assurer, auprès de sa hiérarchie ou de la DSI, du niveau de confidentialité des documents avant de les diffuser, et, le cas échant, des règles prévues pour les Données Sensibles.

La confidentialité des messages est assurée tant que les Utilisateurs respectent les règles de protection des codes d'accès prévus ci-avant au § 3.2.

L'auteur et la confidentialité des messages électroniques ne sont garantis que si l'adresse de mél (e-mail) avec laquelle l'Utilisateur échange des données est équipée d'un dispositif de sécurisation spécifique (signature et chiffrement). Dans ce cas, l'Utilisateur en est averti. Aucune perte ou violation de données personnelles d'un Utilisateur du fait de l'utilisation par ce dernier d'une adresse de mél non sécurisée, depuis la messagerie électronique du Groupe, ne saurait engager la responsabilité du Groupe.

7. REGLES D'UTILISATION D'INTERNET

7.1 UN USAGE RESPONSABLE

L'accès à Internet est accordé aux Utilisateurs en fonction de leurs besoins professionnels.

7.1.1 Navigation

Seuls ont vocation à être consultés les sites Internet présentant un lien direct et nécessaire avec l'activité professionnelle, sous réserve que la durée de connexion n'excède pas un délai raisonnable et présente une utilité au regard des fonctions exercées ou des missions à mener.

Il est rappelé que toutes les activités de l'Utilisateur ainsi que les données le concernant (sites consultés, messages échangés, données fournies à travers des formulaires, données collectées à l'insu de l'Utilisateur, etc.) peuvent être enregistrées par des tiers, analysées pour en déduire ses centres d'intérêt, les préoccupations du Groupe, etc., et utilisées à des fins commerciales ou autres.

En outre, Internet étant un média non sécurisé, il est strictement interdit à un Utilisateur de faire circuler sur Internet des informations confidentielles du Groupe (notamment des Données Sensibles) sans l'autorisation préalable et écrite de sa hiérarchie et de la DSI.

Le Groupe peut interdire et bloquer aux Utilisateurs l'accès à certains sites Internet, notamment les sites reconnus comme illicites, contraires à l'ordre public ou aux bonnes mœurs. A contrario, la classification des sites étant imparfaite, le fait qu'un site ne soit pas bloqué par le Groupe ne signifie pas qu'il soit licite et que sa consultation soit autorisée.

Par souci de respecter le Décret du 23 mai 2006 sur la cybercriminalité, parce que sa responsabilité peut être engagée du fait d'un usage d'Internet contraire aux bonnes mœurs et pouvant revêtir le caractère d'une infraction pénale, et pour maintenir le bon fonctionnement du Système d'Information, le Groupe dresse une liste d'activités prohibées.

Ainsi il est interdit d'utiliser Internet en vue de :

- la diffusion ou le téléchargement de données protégées par le droit d'auteur, en violation des lois protégeant le droit d'auteur;
- la consultation de sites de jeux ou de sites Internet dont le contenu est susceptible de porter atteinte à la dignité d'autrui, notamment la consultation de sites racistes, révisionnistes, érotiques, pornographiques, pédophiles; de même que les sites prônant la discrimination sur base du sexe, de l'orientation sexuelle, du handicap, de la religion, des convictions philosophiques ou politiques d'une personne ou d'un groupe de personnes;
- charger ou transmettre sciemment des fichiers contenant des virus ou des données altérées,
- développer son propre site Internet,
- harceler, menacer ou injurier et, de manière générale, violer des droits en vigueur.

Et l'utilisation d'Internet est tolérée, seulement dans la mesure où elle ne nuit pas à l'efficacité au travail (ou « hors temps de travail »), pour les activités suivantes :

- la participation à un forum de discussion ou de rencontre ou « newsgroup », qui ne soit pas professionnel comme prévu ci-après au §8.2;
- la commande de biens et services destinés à la vie privée (biens de consommation, placements boursiers…);
- écouter la radio ou de regarder la télévision en ligne,

7.1.2 Les messageries personnelles

Un accès raisonnable à une messagerie personnelle par l'Utilisateur est toléré, étant précisé qu'elle relève de la responsabilité de ce dernier. Toute intrusion de virus dans le Système d'Information par le biais d'une messagerie personnelle d'un Utilisateur engagera la responsabilité de celui-ci.

7.1.3 Les blogs et forums de discussions, les messageries instantanées et les réseaux sociaux

Pendant le temps de travail, l'accès à des sites Internet de réseaux sociaux, notamment de type « Facebook », est réservé à un usage professionnel. Il est précisé que ces sites constituent des espaces publics. La liberté d'expression y est garantie dans la limite du respect des dispositions légales concernant la communication publique.

L'utilisation de forums de discussion ou de blogs au moyen des Ressources Informatiques de Le Groupe n'est autorisée que pour un usage strictement professionnel.

Dans ce cas, l'Utilisateur participant à un forum au moyen des Ressources Informatiques du Groupe fera figurer en bas de chacun des messages publiés la mention suivante « Le contenu de ce message n'engage que son auteur et en aucun cas le Groupe SEGULA Technologies ». Dans ce cadre, la diffusion de Données Sensibles constitue un manquement déjà évoqué au § 5.4.

L'utilisation des services de messagerie instantanée publics (« chat ») de type MSN ou Skype est interdite, aussi bien pour un usage personnel que professionnel, au moyen des Ressources Informatiques. En revanche, le Groupe met à la disposition des Utilisateurs qui en ont le besoin un outil de messagerie instantanée interne et interconnecté avec les messageries instantanées de certains partenaires.

7.1.4 Les téléchargements

L'Utilisateur s'engage à limiter les téléchargements à ceux strictement professionnels et vraiment utiles pour l'exécution de sa mission.

Les téléchargements de logiciels ou d'exécutables doivent être approuvés par la DSI, et respecter les droits de propriété intellectuelle et de protection des logiciels.

L'utilisation des services de partage de type Megaupload, Kazaa ou eMule est interdite depuis les Ressources Informatiques du Groupe, aussi bien pour un usage personnel que professionnel.

La DSI se réserve la possibilité d'effacer du Système d'Information toute trace de logiciels, d'œuvres ou de tout autre type de contenu reproduit en violation des droits d'autrui.

7.2 MODALITES D'ACCES A INTERNET

L'Utilisateur s'engage à n'utiliser Internet, s'agissant de son activité dans les locaux du Groupe, qu'à partir des moyens d'accès réseau mis à sa disposition par le Groupe.

7.3 UTILISATION DE TERMINAUX PERSONNELS

La connexion au Système d'Information pour la consultation de la messagerie Groupe est toléré depuis les terminaux personnels de l'Utilisateur (tels que, sans que cette liste soit limitative, ordinateur, Smartphone…), sous réserve que la DSI ait agréé une telle connexion. Dans ce cas l'Utilisateur s'engage à prendre toutes précautions pour s'assurer de la protection et de la

sécurité des Données (notamment en termes de protection anti-virus et de confidentialité) sur ses terminaux.

8. AUDIT ET CONTROLE

La gestion technique des réseaux et des fichiers, et en particulier la gestion de la sécurité, exige que la DSI puisse prendre connaissance des fichiers et des flux. Les moyens de contrôle que le Groupe est amené à mettre en place visent en priorité à maintenir la qualité de service ainsi qu'à contrôler le respect des règles de bon usage et, ceci, dans le cadre de la législation applicable et notamment de la Loi « Informatique et Libertés ».

Le contrôle des fichiers a pour objectif :

- l'entretien du Système d'Information et la détection préventive de virus (anti-spam, spyware…),
- la prévention de l'encombrement des serveurs de données,
- le contrôle du respect des règles définies par la présente Charte.

Le contrôle de l'utilisation d'internet a pour objectif :

- l'optimisation de la bande passante,
- la prévention de la mise en péril des systèmes notamment par l'importation de virus,
- la prévention de l'encombrement du réseau,
- le contrôle du respect des règles définies par la présente Charte.

Le contrôle de la messagerie a pour objectif :

- la sauvegarde des messages, mais uniquement à des fins de restauration,
- le suivi de route (cheminement) des courriers et l'optimisation des performances,
- l'entretien du système et la détection préventive de virus (anti-spam, spyware…),
- la prévention de l'encombrement du serveur messagerie,
- le contrôle du respect des règles définies par la présente Charte.

8.1 L'ACCES AUX FICHIERS

Sauf preuve contraire, tout fichier créé et stocké à l'aide de l'outil informatique mis à disposition du salarié par le Groupe est présumé professionnel.

Des vérifications et des audits réguliers pourront être effectués par le Groupe, dans les limites prévues par la loi et la jurisprudence.

Le Groupe pourra les ouvrir en dehors de la présence de l'Utilisateur sauf si ce dernier les a identifiés comme étant « personnel ».

Par exception à ce qui précède, l'accès à un fichier situé dans un dossier « PRIVE » ou « PERSONNEL » d'un Utilisateur est autorisé s'il a pour objet de faire cesser un trouble grave pour le Groupe (ex : un téléchargement illicite ou portant atteinte à l'intégrité des Ressources Informatiques).

8.2 LES TRACES D'UTILISATION DU SYSTEME D'INFORMATION

Tout Utilisateur a droit au respect de ses données privées. Toutefois, il doit être conscient que les systèmes informatiques enregistrent et peuvent mémoriser les transactions et les informations de connexion.

Le Groupe a mis en place des procédures pour superviser l'usage des Ressources Informatiques.

L'objectif est de maintenir la bonne qualité du service en contrôlant le respect des règles de bon usage. Les abus ont des conséquences négatives pour tous les Utilisateurs.

Les traces de l'utilisation d'Internet par un Utilisateur comportent la liste des sites consultés, la durée de connexion, l'adresse de l'équipement terminal utilisé. Des statistiques mensuelles non nominatives sont constituées.

Une sanction disciplinaire peut être prononcée contre un Utilisateur, sur la base des données ainsi collectées, si leur analyse permet de démontrer que ce dernier a commis une faute.

Le Groupe se réserve le droit de conserver les fichiers de journalisation des traces de connexion globales pendant une période d'1 (un) an.

9. EVOLUTION

La présente Charte entre initialement en vigueur le 1er Octobre 2012.

La présente Charte a été rédigée dans l'intérêt de chacun des Utilisateurs. Elle pourra être mise à jour par le Groupe pour tenir compte de l'évolution constante de l'environnement et des techniques informatiques.

Je, soussigné(e) :

Salarié(e) de la société :

Atteste avoir reçu la présente Charte d'utilisation du Systèmes d'Information du Groupe Segula Technologies et m'engage à la respecter en tout point.

Fait à : , le :

Signature