CHARTE D'UTILISATION DES MOYENS DE COMMUNICATION ELECTRONIQUE

*Les mots ou expressions définis dans le glossaire sont suivis d'un astérisque**

Les nouvelles technologies de l'information ont permis le développement des moyens de communication électronique* dont Internet qui sont vitaux pour notre entreprise.
La réponse à ces risques repose à la fois sur des moyens techniques, sur le bon usage des moyens de communication et sur la vigilance de tous.

L'application de la présente charte s'inscrit dans le cadre général des grands principes de la vie sociale et professionnelle.
Elle vise à réaliser un équilibre entre les besoins de sécurité de l'entreprise et le respect des libertés individuelles et collectives. Sa mise en œuvre doit permettre à chacun d'exercer sa liberté d'expression, reconnue et protégée par la Loi. L'exercice de cette liberté a également des conséquences et des limites, ce qu'entend rappeler ce texte.
Cette charte précise la responsabilité des utilisateurs*, afin d'instaurer un bon usage des moyens de communication électronique* et leur présente les contrôles effectués sur l'utilisation qu'ils font de ces outils.

1. Objectifs et Champ d'application

L'accès aux moyens de communication électronique de la Société est une ressource commune et accessible aux utilisateurs à des fins professionnelles. La sécurité et la disponibilité de ces moyens dépendent de l'usage qui en est fait par chacun.
La présente charte pose des règles permettant d'assurer la sécurité et la performance du système, de préserver la confidentialité des données, dans le respect des lois en vigueur et des droits et libertés reconnus aux utilisateurs*.
Les règles spécifiques d'utilisation des postes multimédia* connectés à Internet*, mis à disposition des salariés afin qu'ils découvrent cet environnement et se familiarisent avec cette nouvelle technologie, restent applicables.
En raison de l'évolution rapide des technologies, cette charte pourra faire l'objet de modifications.
La charte est portée à la connaissance de toute personne utilisatrice du système d'information* de la Société, qu'elle appartienne ou non au personnel de l'entreprise (stagiaires d'études, intérimaires…). Pour les salariés de sociétés extérieures utilisant ce système, cette communication se fait lors de la conclusion du contrat de prestation de services.
Le prestataire contractant répercutera l'information auprès de ses salariés pour lesquels l'autorisation d'accès spéciale a été accordée, à titre dérogatoire, par la Société. Chaque utilisateur doit s'y conformer.

2. Règles de confidentialité

L'accès aux moyens de communication électronique est soumis à habilitation préalable, après autorisation hiérarchique.
Sur le poste de travail*, cet accès requiert une authentification* de l'utilisateur*. Les moyens d'authentification* (code confidentiel*, carte à puce,…) sont strictement personnels et ne doivent servir qu'à l'usage propre de l'utilisateur*, qui est responsable de leur confidentialité. Lors de l'utilisation de ces moyens, l'utilisateur* doit appliquer les principes généraux de confidentialité des informations qu'il détient, et de protection des informations privilégiées.

3. Règles d'utilisation

L'accès aux moyens de communication électronique est mis à disposition des utilisateurs* à des fins professionnelles.
Il en résulte qu'un message envoyé ou reçu depuis le poste de travail mis à la disposition de l'utilisateur revêt un caractère professionnel. Chaque utilisateur est responsable de l'usage qu'il fait des ressources informatiques mises à sa disposition. En cas de dégradation du matériel et en l'absence de toute négligence ou faute de l'utilisateur, la Société prendra à sa charge le coût du matériel. La responsabilité de l'utilisateur en cas de faits fautifs ne sera engagée que s'ils lui sont personnellement imputables. A cet égard, l'authentification ne constitue que l'un des moyens permettant d'établir l'identité d'un utilisateur. Le non-respect des règles définies dans la présente charte pourra entraîner, pour son auteur, l'application d'éventuelles sanctions disciplinaires, de manière appropriée et proportionnée, conformément à l'échelle des sanctions prévues par le règlement intérieur.
En conséquence, l'utilisateur doit :

- choisir des codes confidentiels* et les garder secrets. En aucun cas, il ne doit les communiquer, sauf nécessité de service et avec l'autorisation écrite de son supérieur hiérarchique.
- s'engager 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,
- activer sa protection d'écran* lorsqu'il quitte son poste de travail*,
- ne pas utiliser ou essayer d'utiliser des comptes* autres que le sien ou masquer sa véritable identité,
- ne pas détourner les moyens de communication électronique, dans le but d'en contourner les moyens de sécurité et de surveillance.

Sauf restrictions particulières définies par la hiérarchie, cet accès peut servir aux relations contractuelles ou commerciales à titre professionnel pour lesquelles il convient de respecter les règles suivantes :

- lorsqu'ils peuvent engager la Société, les échanges utilisant des moyens de communication électronique doivent être validés et approuvés au niveau hiérarchique nécessaire.

3.1. Les règles d'utilisation d'internet.

L'accès à internet est attribué individuellement à certains utilisateurs*.
Seuls ont vocation à être consultés les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle exercée, sous réserve que la durée de connexion n'excède pas un délai raisonnable.
L'utilisateur* doit exercer une vigilance toute particulière à l'égard du contenu des échanges et il lui est interdit, lors de l'utilisation des comptes* et infrastructures fournies par la Société, de :

- Visualiser, télécharger, transmettre ou conserver des contenus* à caractère pornographique, pédophile, raciste, xénophobe, diffamatoire, portant atteinte au respect de la personne humaine et à sa dignité, incitant à la commission d'un délit ou d'un crime, contraires à l'ordre public ou aux bonnes mœurs, attentatoires à l'image de marque interne ou externe de la Société.
- Commettre des actes répréhensibles au regard de la loi applicable, notamment en ce qui concerne la propriété intellectuelle.
- Participer à des jeux d'argent, entretenir des relations commerciales à titre privé.
- Participer à des forums de discussions* sur Internet*, une liste de diffusion ou un service d'échange de fichiers, sauf si ceux-ci sont de nature professionnelle ou à condition de s'y exprimer à titre personnel avec réserve, sans y laisser son adresse.
- Créer ou administrer des services Internet* ou de communication électronique étrangers aux besoins de l'activité professionnelle ou n'ayant pas fait l'objet d'une autorisation par le Responsable de la Sécurité des Systèmes d'Information* (RSSI) dont il dépend. Dans ce cas, les utilisateurs* se rapprocheront de leur hiérarchie pour toute demande nécessitant cette autorisation.
- Transmettre ou publier des informations non publiques ou confidentielles à propos de la Société, de ses filiales, de ses clients ou partenaires, ou de son personnel (sauf si autorisé par la hiérarchie et protégé par des moyens adéquats validés).
- Réaliser une connexion à Internet* par des moyens autres que ceux autorisés à cet usage et mis à disposition du personnel à cet effet.

Les transferts de fichiers volumineux ou l'accès à certaines ressources multimédia peuvent entraîner une surcharge importante des moyens de communication électronique. L'utilisateur* devra veiller à ne pas en surcharger
les infrastructures de manière abusive.

3.2. Les règles d'utilisation de la messagerie.

L'utilisateur doit s'efforcer de rédiger des messages courts et clairs ainsi que de limiter le nombre et la taille des pièces jointes* afin d'éviter de surcharger le réseau. L'utilisateur ne doit jamais écrire un message électronique qu'il s'interdirait d'exprimer oralement ou par un autre moyen (courrier, télécopie, etc…), les propos transmis par ce biais pouvant engager la responsabilité de leur auteur et de la Société.
Il doit utiliser avec discernement les listes de diffusion personnelles ou collectives et éviter l'envoi de copies à un nombre injustifié de destinataires. Il est interdit de transmettre, retransmettre ou publier des messages contribuant à un harcèlement sexuel ou moral, menaces ou insultes et de manière générale contraire aux Lois en vigueur. Il ne doit pas transmettre des messages de type chaînes du bonheur, fausses alertes (*hoaxes** en anglais), rumeurs (informations non vérifiées susceptibles d'induire quelqu'un en erreur).

3.3. L'usage privé.

Un usage raisonnable, à titre privé, des moyens de communication électronique est toléré dans le cadre des nécessités de la vie courante et familiale. Cet usage privé doit être limité et de courte durée afin de ne pas affecter le trafic normal des messages professionnels. Une consultation ponctuelle et dans des limites raisonnables de sites internet est acceptée, sous réserve des interdictions mentionnées au §3.1. S'il est fait usage de cette tolérance, l'utilisateur doit, en outre, dans le corps du message, supprimer toute mention relative à l'employeur ou indication qui pourrait laisser croire que le message est rédigé par ses soins dans le cadre de l'exercice de ses fonctions. L'appréciation du caractère privé d'un message relève de la responsabilité de l'émetteur. Chaque utilisateur* devra en informer ses correspondants lors de la communication de son adresse de messagerie à titre privé. Ces messages relèveront des procédures de contrôle* technique identiques à celles définies au §4.

---

*1 Dans les conditions des articles du Code Pénal garantissant le secret de la correspondance, la Société ne pourra pas prendre connaissance du contenu des messages privés ainsi que des fichiers privés de messagerie*regroupant exclusivement ces derniers. S'il s'avère que des indices précis et concordants démontrent que l'utilisateur se livre à une utilisation malveillante ou abusive, la Société sera en droit d'en tirer toutes les conséquences sur le plan disciplinaire et éventuellement judiciaire. L'usage privé abusif se déduira notamment de la fréquence des messages reçus ou envoyés, du volume des données échangées, du format des pièces jointes et de la durée des connexions.* ***L'Administrateur Réseau doit être contactée dès lors que l'utilisateur* soupçonne une faille de sécurité ou une attaque potentielle sur le système d'information* de la*** *Société. Il ne doit pas se charger de diffuser une alerte lui-même auprès des autres utilisateurs*.*

4. Surveillance et audits

Afin d'assurer la sécurité du système d'information*, de veiller au respect des règles définies à la présente charte, la Société se réserve le droit de surveiller l'utilisation faite des moyens de communication électronique, dans le respect du secret de la correspondance privée définie au §3.3 et plus généralement des limites prévues par la Loi.

4.1. Filtrage

Les utilisateurs* sont informés que des systèmes de filtrage* peuvent être mis en place, en particulier :
- pour les messages entrants et sortants avec un contrôle* antiviral.
- pour les messages dont la taille ou la liste de destinataires est trop importante.
- pour les messages en provenance ou à destination d'un utilisateur* ou d'un Serveur* de messagerie* de nature manifestement hostile (envoi massif de messages, harcèlement d'un utilisateur*…).
- pour bloquer, sur la base d'une liste de « mots clefs », des messages ou l'accès à des sites non autorisés.

Plus généralement, tout filtrage nécessaire pour préserver la sécurité du système d'information peut être mis en œuvre.
Le fonctionnement de ces systèmes de filtrage ressort de la compétence des Administrateurs Systèmes dont la mission est définie au §4.4 de la présente charte.

4.2. Collecte d'information

Dans le respect des principes de transparence et de proportionnalité, l'attention des utilisateurs est attirée sur le fait que les dispositifs de sécurité informatique (pare-feu, systèmes de contrôle des accès…) mis en place par la Société enregistrent les traces d'activités des systèmes. L'utilisateur* est donc informé que les messages émis ou reçus sont conservés, de même que les traces* suivantes :

- liste des ressources* auxquelles l'utilisateur a eu accès sur Internet* avec les paramètres techniques de connexion (avec notamment l'identifiant de compte* de l'utilisateur*, date et heure, volume des données transmises…),
- date et heure des authentifications* des utilisateurs* sur les systèmes d'accès aux moyens de communication électronique,
- liste des paramètres techniques nécessaires à la gestion des services de messagerie électronique (identification du compte de l'utilisateur, coordonnées du destinataire, date et heure, volume, format et nature des pièces jointes,…),
- Les traces et messages pourront être conservés pendant une durée maximale d'un an, sauf si des dispositions légales ou réglementaires venaient à imposer aux entreprises des délais de conservation plus importants.

4.3. Caractéristiques

Société peut procéder à des audits à caractère nominatif sur les enregistrements informatiques de l'entreprise, suite à un dysfonctionnement, une alerte de sécurité ou une présomption d'une utilisation non conforme des moyens de communication, sous réserve du respect du secret de la correspondance privée mentionnée au §3.3.
En ce cas, les constatations matérielles ont pour but de relever les diverses circonstances qui éclaireront l'entreprise sur l'éventuelle réalisation d'un fait fautif et sur l'identité de son auteur.

4.4. Le rôle de l'Administrateur Réseau

L'Administrateur Réseau assure le fonctionnement normal et la sécurité des réseaux et systèmes.
En conséquence, par sa fonction même, il a accès à l'ensemble des informations relatives aux utilisateurs.
Il est tenu par un devoir de confidentialité. Dans ce cadre, ils ne doivent pas divulguer ces informations lorsqu'elles sont couvertes par le secret de la correspondance privée ou relèvent de la vie privée des utilisateurs et ne mettent en cause ni le bon fonctionnement technique des applications, ni la sécurité, ni l'intérêt de l'entreprise.

4.5 Mesures techniques et administratives

Par mesure technique ou administrative, l'accès aux moyens de communication électronique pourra être suspendu, restreint ou supprimé, individuellement ou collectivement quand cela est nécessaire, notamment pour le maintien de la bonne marche ou de l'intégrité du système d'information* de la Société.

Glossaire

Antiprogramme
Programme ou partie de programme destiné à perturber, altérer ou détruire tout ou partie des éléments logiques indispensables au bon fonctionnement d'un système informatique.

Authentification :
Processus permettant de vérifier l'identité d'un utilisateur*. L'authentification d'un Utilisateur* par une application se fait souvent au moyen d'un code confidentiel*.

Cheval de Troie :
Antiprogramme* qui introduit dans une séquence d'instructions normales, prend l'apparence d'un programme valide contenant en réalité une fonction illicite cachée, grâce à laquelle les mécanismes de sécurité du système informatique sont contournés, ce qui permet la pénétration par effraction dans des fichiers pour les consulter, les modifier ou les détruire.

CNIL :
Commission Nationale Informatique et Libertés.

Chiffrement :
Opération par laquelle est substitué, à un texte en clair, un texte inintelligible, inexploitable pour quiconque ne possède pas la clé permettant de le ramener à sa forme initiale.

Code confidentiel :
Séquence de lettres, de chiffres et de symboles, permettant à un utilisateur* de s'authentifier auprès d'un service ou d'une application.

Compte utilisateur :
Identité et ensemble de droits d'accès attribués à un utilisateur d'un système informatique.

Contenu :
Informations.

Contrôle (des données) :
Opération servant à vérifier la qualité ou l'intégrité des données.

Fichier de messagerie :
Fichier créé par le logiciel de messagerie pour classer, stocker ou archiver un ensemble de messages.

Filtrage :
Action consistant à appliquer sur des flux d'information un ensemble de règles autorisant ou interdisant certains types de flux.

Forum :
Service offert par un serveur* d'information dans un réseau comme Internet* et qui permet à un groupe de personnes d'échanger leurs opinions, leurs idées sur un sujet particulier, en direct ou en différé, selon des formules variées.

Hoax (pl hoaxes) (mot anglais signifiant *canular*) :
Message électronique émis dans l'intention de saturer les systèmes de messagerie*, en incitant ses destinataires à le rediffuser en abusant de leur bonnefoi.

Http :
Hyper Text Transfert Protocol. Protocole de communication majeur du Web*, permettant d'accéder aux ressources* hyper-texte disponibles sur le Web*.

Internet :
Réseau mondial de télécommunication, permettant, à partir d'ordinateurs interconnectés, d'accéder à plusieurs types d'applications comme le web*, le courrier électronique, les forums* de discussion, et le transfert de fichiers, logiciels ou données.

Messagerie électronique :
Service de transmission de messages géré par ordinateur, fournissant aux utilisateurs*
autorisés les fonctions de saisie, de distribution et de consultation de messages. Les utilisateurs* de ce service disposent d'une adresse de messagerie électronique, qui sert à leur adresser des messages.

Moyens de communication électronique :
Ensemble des outils et services mis à disposition des utilisateurs* du système d'information* pour communiquer.

Les moyens de communication électronique sont la messagerie électronique*, les services d'accès à Internet* et les outils de travail en commun sur Intranet.

Outils de travail en commun sur Intranet :
Services qui permettent à des utilisateurs*reliés par un réseau de travailler en collaboration sur un même projet.

Pièce jointe :
Fichier envoyé en accompagnement d'un message électronique. Chaque pièce jointe a une taille correspondant à celle du fichier original.

Piste d'audit :
Ensemble de traces* de l'activité des utilisateurs*, permettant de retrouver a posteriori quelles actions ont été effectuées par les utilisateurs*.

Poste de travail :
Ordinateur connecté au réseau interne Société Générale, mis à disposition des utilisateurs* pour effectuer leur travail.

Protection d'écran :
Outil souvent intégré à l'économiseur d'écran, permettant à un utilisateur* connecté au système d'information* d'empêcher* l'utilisation de son compte* pendant une absence de courte durée.

Ressource Internet :
Contenu* ou service accessible par Internet*. En l'état actuel des technologies, il peut s'agir d'une page web*, d'un service en ligne, d'un flux vidéo…

Serveur :
Système informatique qui héberge un ou des services.

Système d'information :
Dans le système informatique d'une entreprise, ensemble de tous les éléments qui contribuent au traitement et à la circulation de l'information dans l'entreprise (base de données, logiciels d'application, procédures, documentation, etc.), y compris le système informatique proprement dit (unité centrale de traitement, périphériques, système d'exploitation, etc.).

Téléchargement :
Action consistant, pour un utilisateur*, à transférer une ressource Internet* depuis l'endroit où elle est mise à disposition vers une ressource interne accessible à l'utilisateur*.

Trace :
Enregistrement permettant de mémoriser un événement survenu dans un système d'information*. Les traces peuvent servir à la surveillance technique des applications ou bien au contrôle de l'activité des utilisateurs*.
L'enregistrement des traces est alors une piste d'audit*.

Utilisateur :
Personne habilitée à se connecter au système d'information* (i.e. possédant un compte*).

Virus :
Antiprogramme dont l'exécution est déclenchée lorsque le vecteur auquel il a été attaché clandestinement est activé, qui se recopie au sein d'autres programmes ou sur des zones systèmes lui servant à leur tour de moyen de propagation, et qui produit les actions malveillantes pour lesquelles il a été conçu.

Web :
Appelé exactement World Wide Web – W.W.W. Système permettant d'accéder aux ressources d'Internet*, basé sur le protocole http*.