

GRANDISCOUTURE

Charte d'utilisation des ressources informatiques

GRANDISCOUTURE

Table des matières

Article I.	PROTECTION DES DONNEES A CARACTERE PERSONNEL.....	2
Article II.	LE CHAMP D'APPLICATION DE LA CHARTE.....	3
Article III.	LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION	3
Section 3.01	Les modalités d'intervention du service de l'informatique interne	3
Section 3.02	L'authentification.....	4
Section 3.03	Les règles de sécurité	4
Article IV.	LES MOYENS INFORMATIQUES	5
Section 4.01	Configuration du poste de travail.....	5
Section 4.02	Equipements nomades et procédures spécifiques aux matériels de prêt.....	5
(a)	4.2.1 Equipements nomades.....	5
(b)	Procédures spécifiques aux matériels de prêt	6
(c)	Internet	6
Section 4.03	Messagerie électronique.....	6
(a)	Conditions d'utilisation.....	6
(b)	Consultation de la messagerie.....	7
(c)	Courriel non sollicité.....	8
Section 4.04	Téléphone.....	8
Section 4.05	L'utilisation des outils informatiques par les représentants du personnel	8
Article V.	L'ADMINISTRATION DU SYSTEME D'INFORMATION	9
Section 5.01	Les systèmes automatiques de filtrage.....	9
Section 5.02	Les systèmes automatiques de traçabilité	9
Section 5.03	Gestion du poste de travail.....	9
Article VI.	PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR ...	10
Article VII.	RESPONSABILITES- SANCTIONS	10
Article VIII.	INFORMATION DES SALARIES	10
Article IX.	ENTREE EN VIGUEUR DE LA CHARTE.....	11
ANNEXE I :	DISPOSITIONS LEGALES APPLICABLES	12
ANNEXE II :	QUELQUES DEFINITIONS.....	12

GRANDISCOUTURE

INTRODUCTION

La Société met en œuvre un système d'information et de communication nécessaire à l'exercice de son activité. Elle met ainsi à disposition de ses collaborateurs des outils informatiques, et de communication sur l'ensemble de l'entreprise.

La présente charte définit les conditions d'accès et les règles d'utilisation des moyens informatiques et des ressources extérieures via les outils de communication de la Société. Elle a également pour objet de sensibiliser les utilisateurs aux risques liés à l'utilisation de ces ressources en termes d'intégrité et de confidentialité des informations traitées. Ces risques imposent le respect de certaines règles de sécurité et de bonne conduite. Le comportement des utilisateurs (l'imprudence, la négligence voire la malveillance dans les cas extrêmes) peuvent en effet avoir des conséquences graves de nature à engager la responsabilité civile et/ou pénale de l'utilisateur ainsi que celle de la société.

Article I. PROTECTION DES DONNEES A CARACTERE PERSONNEL

La loi n°78-17 du 6 janvier 1978 modifiée en 2004 relative à l'informatique, aux fichiers et aux libertés définit les conditions dans lesquelles des traitements de données à caractère personnel peuvent être effectués. Elle ouvre aux personnes concernées par les traitements un droit d'accès et de rectification des données enregistrées sur leur compte.

La Société a désigné un correspondant à la protection des données à caractère personnel : Responsable de l'Administration des Ressources Humaines, des Relations Sociales et Juridique. Ce dernier a pour mission de veiller au respect des dispositions de la loi n°78-17 du 6 janvier 1978 modifiée.

Il est obligatoirement consulté par le responsable des traitements, à savoir le Responsable Informatique, préalablement à leur création.

Le Responsable Informatique recense dans un registre la liste de l'ensemble des traitements de données à caractère personnel de la société au fur et à mesure de leur mise en œuvre. Cette liste est tenue à disposition de toute personne en faisant la demande.

GRANDISCOUTURE

Le correspondant veille au respect des droits des personnes (droit d'accès, de rectification et d'opposition). En cas de difficultés rencontrées lors de l'exercice de ces droits, les personnes concernées peuvent saisir la CNIL : TSA 80715, 3, PL de Fontenoy, 75334 Paris.

Article II. LE CHAMP D'APPLICATION DE LA CHARTE

La présente charte s'applique à tout utilisateur du Système d'Information et de communication de l'entreprise pour l'exercice de ses activités professionnelles. L'utilisation à titre privé de ces outils est tolérée, mais doit être raisonnable et ne pas perturber le bon fonctionnement du service.

La charte est à considérer comme une annexe du règlement intérieur.

Elle est systématiquement remise à tout nouvel arrivant.

Toutes actions de communication internes sera organisées à l'initiative du service informatique afin d'informer les utilisateurs des bonnes pratiques, par exemple :

- Réinitialisation du Mot de passe de messagerie
- Réinitialisation du Mot de passe de connexion à sa session Microsoft

Article III. LES REGLES D'UTILISATION DU SYSTEME D'INFORMATION

Chaque utilisateur accède aux outils informatiques nécessaires à l'exercice de son activité professionnelle dans les conditions définies par le Directeur du service.

Le service informatique s'assure de la cohérence des droits accordés par rapport à la fonction et a pour mission de veiller à la confidentialité générale des données.

Section 3.01 Les modalités d'intervention du service de l'informatique interne

Le service informatique assure le bon fonctionnement et la sécurité des réseaux, des moyens informatiques et de communication de l'entreprise.

Ce service dispose d'outils techniques afin de procéder aux investigations et au contrôle de l'utilisation des systèmes informatiques mis en place.

Le service informatique a accès à l'ensemble des données techniques mais s'engagent à respecter les règles de confidentialité applicables aux contenus des documents.

GRANDISCOUTURE

Ils sont assujettis au devoir de réserve et sont tenus de préserver la confidentialité des données qu'ils sont amenés à connaître dans le cadre de leurs fonctions.

Section 3.02 L'authentification

L'accès aux ressources informatiques repose sur l'utilisation d'un nom de compte ("login" ou identifiant) fourni à l'utilisateur lors de son arrivée. Un mot de passe est associé à cet identifiant de connexion. Les moyens d'authentification sont personnels et confidentiels.

Le mot de passe est créé par le service informatique, il est de la responsabilité des utilisateurs de le modifier à leur arrivée ou si jamais il a été communiqué à un collègue.

Il ne doit comporter ni le nom, prénom ni l'identifiant d'ouverture de la session de travail. Il doit être renouvelé le plus régulièrement possible sous la responsabilité de l'utilisateur (tous les 3 mois).

Section 3.03 Les règles de sécurité

Tout utilisateur s'engage à respecter les règles de sécurité suivantes :

- Signaler au service informatique toute violation ou tentative de violation suspectée de son compte réseau et de manière générale tout dysfonctionnement ;
- Ne jamais confier son identifiant/mot de passe ;
- Ne jamais demander son identifiant/mot de passe à un collègue ou à un collaborateur ;
- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Ne pas modifier les paramètres du poste de travail ;
- Ne pas copier, modifier, détruire les logiciels propriétés mis à disposition au sein de l'entreprise ;
- Verrouiller son ordinateur dès qu'il quitte son poste de travail ;
- Ne pas accéder, tenter d'accéder, supprimer ou modifier des informations qui ne lui appartiennent pas ;
- Toute copie de données sur un support externe est soumise à l'accord du Directeur de service et doit respecter les règles définies par la société.

En outre, il convient de rappeler que les visiteurs ne peuvent avoir accès au Système d'Information de l'entreprise sans l'accord préalable du service informatique.

GRANDISCOUTURE

Les intervenants extérieurs doivent s'engager à faire respecter la présente charte par leurs propres salariés et éventuelles entreprises sous-traitantes. Dès lors, les contrats signés entre l'entreprise et tout tiers ayant accès aux données, aux programmes informatiques ou autres moyens, doivent comporter une clause rappelant cette obligation.

Article IV. LES MOYENS INFORMATIQUES

Section 4.01 Configuration du poste de travail

La société met à disposition de chaque utilisateur un poste de travail doté des outils informatiques nécessaires à l'accomplissement de ses fonctions. L'utilisateur ne doit pas :

- Modifier ces équipements et leur fonctionnement, leur paramétrage, ainsi que leur configuration physique ou logicielle ;
- Connecter ou déconnecter du réseau les outils informatiques et de communications sans y avoir été autorisé par l'équipe informatique interne ;
- Déplacer l'équipement informatique (sauf s'il s'agit d'un « équipement nomade ») ;
- Nuire au fonctionnement des outils informatiques et de communications.

Toute installation de logiciels supplémentaires est subordonnée à l'accord du service informatique.

Section 4.02 Equipements nomades et procédures spécifiques aux matériels de prêt

(a) 4.2.1 Equipements nomades

On entend par « équipements nomades » tous les moyens techniques mobiles (ordinateur portable, imprimante portable, téléphones mobiles ou smartphones, CD ROM, clé USB etc...). Quand cela est techniquement possible, ils doivent faire l'objet d'une sécurisation particulière, au regard de la sensibilité des documents qu'ils peuvent stocker. L'utilisation de smartphones pour relever automatiquement la messagerie électronique comporte des risques particuliers pour la confidentialité des messages, notamment en cas de perte ou de vol de ces équipements. Quand ces appareils ne sont pas utilisés pendant quelques minutes, ils doivent donc être verrouillés par un moyen adapté de manière à prévenir tout accès non autorisé aux données qu'ils contiennent.

GRANDISCOUTURE

(b) Procédures spécifiques aux matériels de prêt

La mise à disposition d'un matériel spécifique pour la tenue d'une réunion, implique que l'utilisateur est garant de la sécurité des équipements qui lui sont remis et ne doit pas contourner la politique de sécurité mise en place sur ces mêmes équipements.

Le matériel doit être retourné au service informatique à la fin de la période de prêt, toutes anomalies de fonctionnement doit être stipulée de façon à prévenir les pannes.

(c) Internet

Les utilisateurs peuvent consulter les sites internet présentant un lien direct et nécessaire avec l'activité professionnelle.

Toutefois, une utilisation ponctuelle et raisonnable, pour un motif personnel, des sites internet dont le contenu n'est pas contraire à la loi, l'ordre public et ne met pas en cause l'intérêt et la réputation de l'entreprise, est admise.

Section 4.03 Messagerie électronique

(a) Conditions d'utilisation

La messagerie électronique n'est pas destinée à remplacer toute autre forme de communication dans l'entreprise ou avec des tiers.

Chacun doit donc se demander si l'envoi d'un message est bien la forme de communication la plus appropriée à la situation par rapport à l'utilisation des dossiers partagés sur nos serveurs, ou à un échange, réunion, appel téléphonique.

La messagerie mise à disposition des utilisateurs est destinée à un usage professionnel. L'utilisation de la messagerie à des fins personnelles est tolérée si elle n'affecte pas le travail du collaborateur ni la sécurité du réseau informatique de l'entreprise.

Tout message qui comportera la mention expresse ou manifeste de son caractère «personnel» bénéficiera du droit au respect de la vie privée et du secret des correspondances. A défaut, le message est présumé professionnel.

La société s'interdit d'accéder aux dossiers et aux messages identifiés comme «personnel» dans l'objet de la messagerie.

L'utilisation de la messagerie électronique doit se conformer aux règles d'usage définies par le service informatique, et validées par la direction concernée.

GRANDISCOUTURE

Il est ainsi recommandé :

- De limiter le stockage des messages tant pour maintenir le bon fonctionnement du système que pour réduire le risque d'accès de tiers aux informations confidentielles qui y sont contenues ;
- Il convient donc de procéder régulièrement à une vérification des messages reçus ou envoyés pour détruire ceux qui ne présentent plus d'utilité ;
- De contrôler la volumétrie de la messagerie en limitant son nombre d'année ;
- De limiter la taille maximale d'un courriel à 5 Mo lors de l'envoi et de la réception d'un message ;
- De limiter le nombre de destinataires simultanés lors de l'envoi d'un message ;
- De mettre en œuvre un archivage de la messagerie avec l'aide du service informatique.

Le transfert de messages, ainsi que leurs pièces jointes, à caractère professionnel sur des messageries personnelles est soumis aux mêmes règles que les copies de données sur supports externes.

Les collaborateurs peuvent consulter leur messagerie à distance, à l'aide d'un navigateur (webmail). Les fichiers qui seraient copiés sur l'ordinateur utilisé dans ce cadre doivent être effacés dès que possible de l'ordinateur utilisé.

(b) Consultation de la messagerie

En cas d'absence et afin de ne pas interrompre le fonctionnement du service ou de l'activité, le service informatique de la société peut, ponctuellement transmettre au supérieur hiérarchique un message électronique à caractère exclusivement professionnel et identifié comme tel par son objet et/ou son expéditeur (cf. conditions d'utilisation).

Le supérieur hiérarchique n'a pas accès aux autres messages et la personne concernée est informée dès que possible de la liste des messages qui ont été transférés.

En cas d'absence prolongée, le responsable peut demander au service informatique, après accord de son directeur, le transfert des messages reçus.

GRANDISCOUTURE

(c) Courriel non sollicité

La Société dispose d'un outil permettant de lutter contre la propagation des messages non désirés (spam). Aussi, afin de ne pas accentuer davantage l'encombrement du réseau lié à ce phénomène, les utilisateurs sont invités à limiter leur consentement explicite préalable à recevoir un message de type commercial, newsletter, abonnements ou autres, et de ne s'abonner qu'à un nombre limité de listes de diffusion notamment si elles ne relèvent pas du cadre strictement professionnel.

Section 4.04 Téléphone

La société met à disposition des utilisateurs, pour l'exercice de leur activité professionnelle, des téléphones fixes et mobiles.

L'utilisation du téléphone à titre privé est admise à condition qu'elle demeure raisonnable.

Des restrictions d'utilisation des téléphones fixes sont mises en place en tenant compte des missions de chacun. A titre d'exemple, certains postes sont limités aux appels nationaux, d'autres peuvent passer des appels internationaux.

La société s'interdit de mettre en œuvre un suivi individuel de l'utilisation des services de télécommunications. Seules des statistiques globales sont réalisées sur l'ensemble des appels entrants et sortants. Elle vérifie que les consommations n'excèdent pas les limites des contrats passés avec les opérateurs.

La société s'interdit d'accéder à l'intégralité des numéros appelés via l'autocommutateur mis en place et via les téléphones mobiles. Toutefois, en cas d'utilisation manifestement anormale, le service informatique, sur demande de la Direction se réserve le droit d'accéder aux numéros complets des relevés individuels.

Section 4.05 L'utilisation des outils informatiques par les représentants du personnel

Les représentants du personnel comité économique et social (CSE) utilisent, dans le cadre de leur mandat, les outils informatiques qui leur sont attribués pour l'exercice de leur activité professionnelle. Ils disposent d'une adresse électronique dédiée (representants@nomde l'Atelier.fr). Les représentants du personnel sont soumis à la présente charte.

GRANDISCOUTURE

Article V. L'ADMINISTRATION DU SYSTEME D'INFORMATION

Afin de surveiller le fonctionnement et de garantir la sécurité du système d'information, différents dispositifs sont mis en place.

Section 5.01 Les systèmes automatiques de filtrage

A titre préventif, des systèmes automatiques de filtrage permettant de diminuer les flux d'information non souhaitable pour l'entreprise et d'assurer la sécurité et la confidentialité des données qui sont mis en œuvre. Il s'agit notamment du filtrage des sites Internet, de l'élimination des courriels non sollicités, du blocage de certains protocoles (peer to peer, messagerie instantanée hors entreprise....).

Section 5.02 Les systèmes automatiques de traçabilité

Le service informatique opère sans avertissement les investigations nécessaires à la résolution de dysfonctionnements du système d'information ou de l'une de ses composantes, qui mettent en péril son fonctionnement ou son intégrité.

Il s'appuie pour ce faire, sur des fichiers de journalisation (fichiers « logs ») qui recensent toutes les connexions et tentatives de connexions au système d'information. Ces fichiers comportent les données suivantes : dates, IP postes de travail, objet de l'évènement et profil de l'utilisateur. Le service informatique est le seul utilisateur de ces informations qui sont effacées à l'expiration d'un délai de 1 an.

Section 5.03 Gestion du poste de travail

A des fins de maintenance informatique, le service informatique peut accéder à distance à l'ensemble des postes de travail. Cette intervention s'effectue avec l'autorisation orale de l'utilisateur.

Dans le cadre de mises à jour et évolutions du système d'information, et lorsqu'aucun utilisateur n'est connecté sur son poste de travail, le service informatique peut être amené à intervenir sur l'environnement technique des postes de travail.

Il s'interdit d'accéder aux contenus.

GRANDISCOUTURE

Article VI. PROCEDURE APPLICABLE LORS DU DEPART DE L'UTILISATEUR

Lors de son départ, l'utilisateur doit restituer au service de l'informatique les matériels mis à sa disposition.

Il doit préalablement effacer ses fichiers et données privées. Toute copie ou transfert de documents professionnels est strictement interdit sauf autorisation expresse du chef de service. Les comptes et les données personnelles de l'utilisateur sont, en tout état de cause, supprimés dans un délai maximum d'un mois après son départ.

Article VII. RESPONSABILITES- SANCTIONS

Le manquement aux règles et mesures de sécurité et de confidentialité définies par la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner des sanctions après un rappel bienveillant de la part de la Direction et/ou du service informatique.

Elles consistent après avis du Directeur de la personne compétente et de la Direction des Ressources Humaines :

- En un rappel aux fondamentaux sur la base des informations factuelles et objectives transmises par le service informatique, en cas de non-respect des règles énoncées par la charte ;
- En cas de renouvellement ou en cas de gravité de l'atteinte, en des sanctions disciplinaires.

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'information (cf. liste des textes en annexe) est susceptible de sanctions pénales prévues par la loi.

La vigilance et le sens des responsabilités de chacun sont de plus en plus requis compte tenu de l'ensemble des menaces qui pèsent sur l'entreprise.

Article VIII. INFORMATION DES SALARIES

La présente charte est affichée en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié.

Le service informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des nouvelles technologies de l'information et de la communication. Il

GRANDISCOUTURE

informe les utilisateurs régulièrement sur l'utilisation des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise. Chaque utilisateur doit s'informer sur les techniques de sécurité et veiller à maintenir son niveau de connaissance en fonction de l'évolution technologique.

Article IX. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte est applicable à compter du 01 03 2019.

Elle a été adoptée après information et consultation des représentants du personnel.

XXXX

GRANDISCOUTURE

ANNEXE I : DISPOSITIONS LEGALES APPLICABLES

- Directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données
- Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés modifiée par la loi n°2004-801 du 6 août 2004
- Le règlement n° 2016/679, dit règlement général sur la protection des données, est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel
- Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique
- Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique (LCEN)
- Loi n°94-361 du 10 mai 1994 sur la propriété intellectuelle des logiciels

ANNEXE II : QUELQUES DEFINITIONS

- « utilisateur » : toute personne autorisée à accéder aux outils informatiques et aux moyens de communication de l'entreprise et à les utiliser (collaborateurs, stagiaires, intérimaires, personnels de sociétés prestataires, visiteurs occasionnels).
- « outils informatiques et de communication » : tous les équipements informatiques de télécommunications et de reprographie de l'entreprise.