Projet SAS

10/01/2017

NICOLAS BOILLAUD
CHARLES GNECCHI
ALEXIS LEGRAND

PowerTech

Table des matières

.

I. Introduction

Notre directeur technique nous demande d'effectuer les actions suivantes :

-Réaliser une note de synthèse sur les problématiques du point de vue de la loi d'utilisation des outils informatiques en entreprise

-Etablir un plan de sécurisation des données

-Engagement qualité

-Mémo pour la conduite à tenir chez le client

II. Notre entreprise

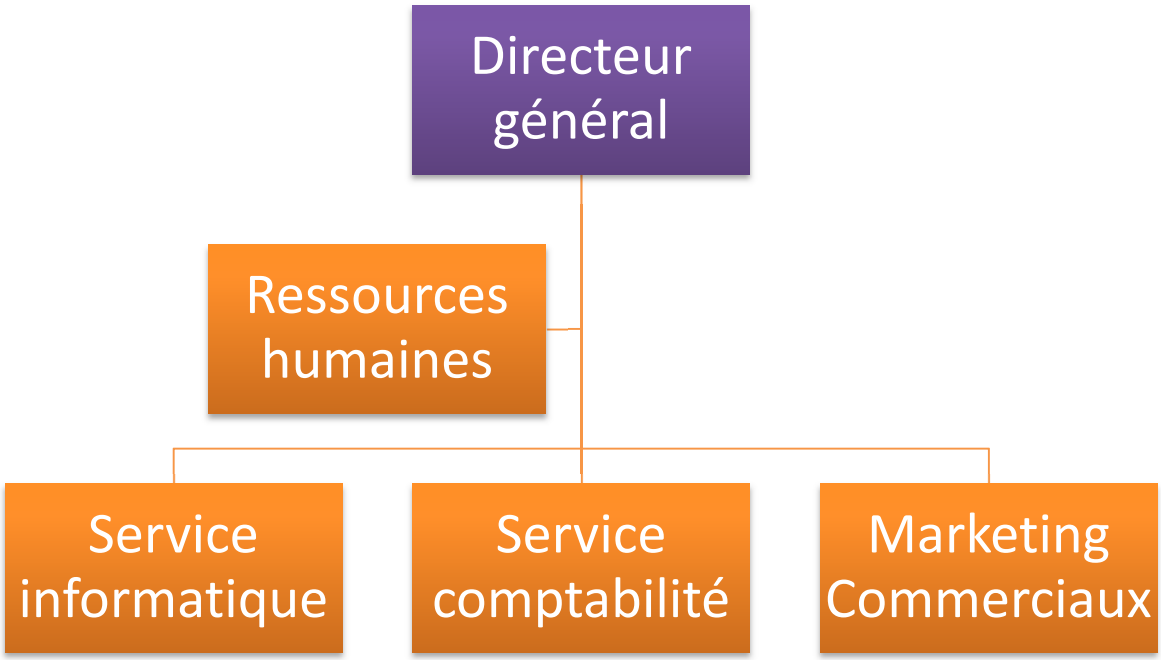
Présentation

Notre entreprise "PowerTech" a été créée en 1998 et est composée de 45 salariés partagés en différents services.

Prestations réalisées

La maintenance des systèmes d'information, l'installation de réseau locaux et d'échange de donnés ainsi que le support sont les prestations que nous mettons à disposition de nos clients.

Organigramme



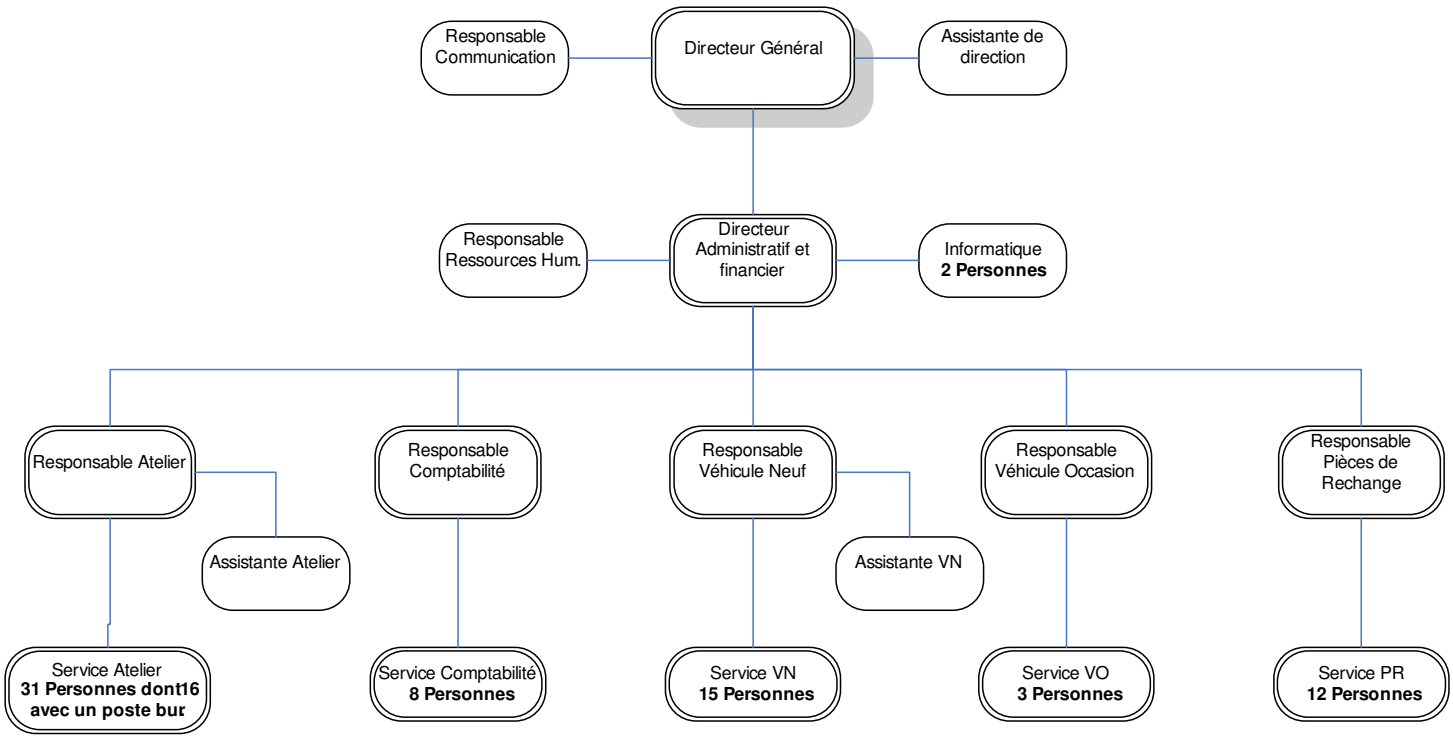
III. Présentation client

AutoConcept est un concessionnaire automobile, disposant d'un parc informatique d'environ 75 postes.

Elle souhaite externaliser les prestations informatiques qui sont actuellement faites par deux informaticiens internes à l'entreprise.

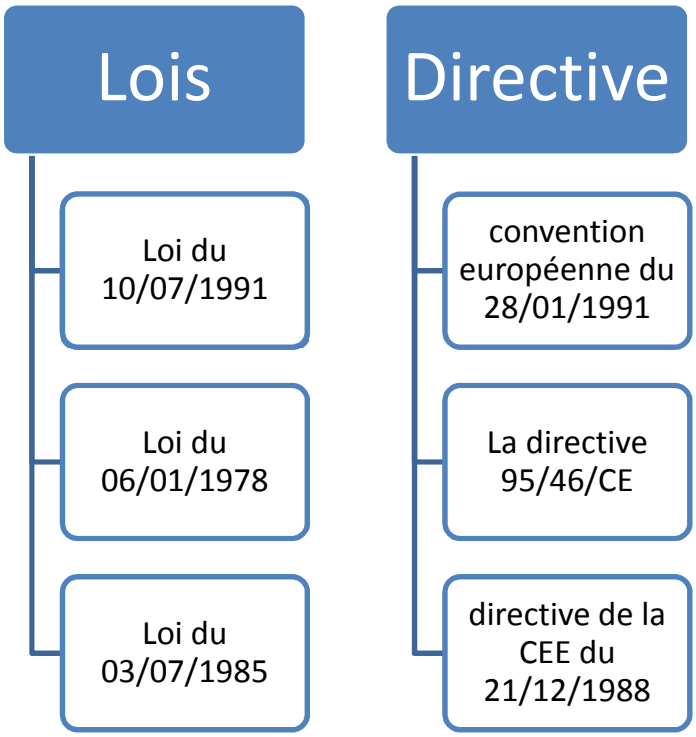
Notre directeur nous charge de réaliser une partie de l'étude avant-vente et nous annonce qu'en cas d'obtention du marché, l'un des deux informaticiens de l'entreprise « AutoConcept » sera recruté.

Organigramme de l'entreprise "AutoConcept"



IV. Cadre juridique

A. Les lois et directives informatiques



Loi du 06/01/1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour objet de protéger les libertés individuelles susceptibles d'être menacées par l'utilisation de l'outil informatique.

Loi du 03/07/1985 relative aux droits d'auteur et aux droits des artistes-interprètes et des entreprises audiovisuelles. Elle interdit à l'utilisateur toute reproduction d'un logiciel sauf pour la création d'une sauvegarde.

Loi du 10/07/1991 relative au secret des correspondances par les voies de communication électroniques.

La convention européenne du 28/01/1991 relative à la protection des personnes à l'égard du traitement informatisé des données à caractère personnel. Elle définit les principes de base de la protection des données. Elle règle la coopération entre Etats pour la mise en œuvre de la Convention, en particulier l'assistance qu'un Etat membre doit prêter aux personnes concernées ayant leur résidence à l'étranger.

La directive 95/46/CE relative à la protection des données personnelles et à la libre circulation de ces données. Cette directive vise à réduire les divergences entre les législations nationales sur la protection des données afin de lever tout obstacle à la libre circulation des données à caractère personnel à l'intérieur de l'Union Européenne.

La directive de la CEE du 21/12/1988 sur l'harmonisation de la protection juridique des logiciels protège les droits d'auteur, elle interdit en particulier à l'utilisateur d'un logiciel toute reproduction autre que l'établissement d'une copie de sauvegarde.

B. Informations sur l'utilisation de l'outil informatique

La charte d'utilisation de l'outil informatique règlemente (présente en annexe) :

- Le respect du matériel mis à disposition.
- L'utilisation de logiciels et de fichiers personnels.
- La sécurité des postes l'accès au réseau de l'entreprise.
- L'utilisation d'E-Mails, la navigation Internet.

La signature de cette charte est obligatoire pour pouvoir recevoir les identifiants de connexion au réseau de l'entreprise. Une fois signée l'utilisateur s'engage au respect de celle-ci.

C. Filtrage

Obligations de moyen

- L'entreprise doit mettre en œuvre les moyens nécessaires pour interdire l'accès à des sites illégaux, notamment en ce qui concerne les téléchargements de fichiers ou logiciels piratés via une solution de filtrage de contenus Web notamment.

Obligations de conservation des logs

- Lors de la mise en place d'une solution de filtrage Internet, l'entreprise doit s'engager à conserver les données de connexion (LOG) pendant 1 an.

Obligations de déclaration à la CNIL

- Lorsque la solution de filtrage Internet mise en place collecte des informations nominatives, il est nécessaire de faire une déclaration à la CNIL. En revanche, cette déclaration n'est pas obligatoire si le filtre Internet ne permet pas un contrôle individualisé des salariés.

D. Déclarations obligatoires

Tout fichier ou traitement automatisé contenant des informations à caractère personnel doit être déclaré avant sa création, en ligne ou par courrier adressé à la Commission nationale de l'informatique et des libertés (CNIL) sous forme d'une :

Déclaration normale pour les fichiers qui concernent la vie privée ou les libertés individuelles des personnes.
Déclaration simplifiée valant engagement de conformité, pour les fichiers qui ne portent pas atteinte à la vie privée et aux libertés individuelles des personnes.

E. Autorisation préalable obligatoire

Une autorisation préalable de la CNIL est obligatoire pour les fichiers qui présentent des risques particuliers d'atteinte aux droits et aux libertés :

Les données enregistrées portant sur des informations sensibles, biométriques ou génétiques, etc.

Les fichiers ayant une finalité particulière (exemple : une étude statistique)

Les transferts de données hors de l'Union européenne.

La demande d'autorisation fait l'objet d'un examen approfondi de la part de la CNIL, qui a 2 mois pour se prononcer. Une fois la délibération prise, la Cnil doit la notifier dans les 8 jours au responsable de traitement.

Sanctions : Si le responsable des données n'effectue par les déclarations auprès de la CNIL, il peut être condamné à 5 ans d'emprisonnement et 300 000 € d'amende.

F. Obligation d'information

L'exploitant de données personnelles, c'est-à-dire l'entreprise, doit recueillir l'accord des salariés après les avoir informé :

De l'identité du responsable du fichier,

De la finalité du traitement des données,

De leurs droits d'accès, de rectification, d'interrogation et d'opposition aux informations collectées.

Des transmissions des données.

L'objectif de la collecte d'informations doit être précis et les données en accord avec cette finalité.

Sanctions : Le non-respect du droit des personnes est puni à hauteur de 1 500 € par infraction et de 3 000 € lors d'une récidive.

G. Obligation de sécurité et de confidentialité

Le responsable du traitement des données est dans l'obligation d'assurer la confidentialité des données. Il doit de ce fait mettre en œuvre des mesures de sécurité des locaux et des systèmes d'information pour empêcher que les fichiers soient déformés, endommagés, ou que des personnes non autorisées y aient accès.

L'accès aux données est réservé uniquement aux personnes désignées ou à des tiers qui détiennent une autorisation spéciale et ponctuelle tels que le service des impôts ou la police.

Le responsable des données est tenu de fixer une durée raisonnable de conservation des informations personnelles.

Sanctions : Si ces obligations ne sont pas respectées, l'entreprise et son responsable des données encourt 5 ans d'emprisonnement et une amende de 300 000 €.

H. Sanctions

Outre les sanctions pénales (amende, emprisonnement), le manquement de l'entreprise aux obligations de protection des données personnelles peut entraîner de la part de la CNIL :

Un avertissement
Une amende
Le verrouillage des données pendant 3 mois
Une injonction d'arrêter le traitement des données
Un retrait de l'autorisation de la Cnil

V. Sécurisation des données

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre par l'intermédiaire de leur direction des systèmes d'information (DSI) ou du responsable informatique.

A. Confidentialité

Adopter une politique de mot de passe

L'accès à un poste informatique ou à un fichier par identifiant et mot de passe est la première des protections. Le mot de passe doit être individuel et rester secret. La DSI devra mettre en place une politique de gestion des mots de passe rigoureuse. Le mot de passe comportera au minimum 8 caractères incluant au moins un chiffre ou caractère spécial et devant être renouvelé tous les 90 jours.

Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs, et non « génériques », afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants.

Identifier et vérifier les droits d'accès

L'accès aux données personnelles traitées dans un fichier doit être limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. Il est de fait nécessaire de mettre en place au sein de l'entreprise plusieurs profils d'habilitation.

Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des divers sous-traitants du système d'information doivent présenter des garanties suffisantes en termes de sécurité et de confidentialité à l'égard des données auxquels ceux-ci peuvent avoir accès. La loi impose ainsi qu'une clause de confidentialité soit prévue dans les contrats de sous-traitance.

B. Disponibilité

Anticiper le risque de perte

Pour éviter la perte de données sensibles et cruciales à l'activité de l'entreprise (Exemple : Panne matérielle, dégâts des eaux, incendie), il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et faisant l'objet de sauvegardes régulières.

Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs. Les serveurs hébergeant des données importantes pour l'activité doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne.

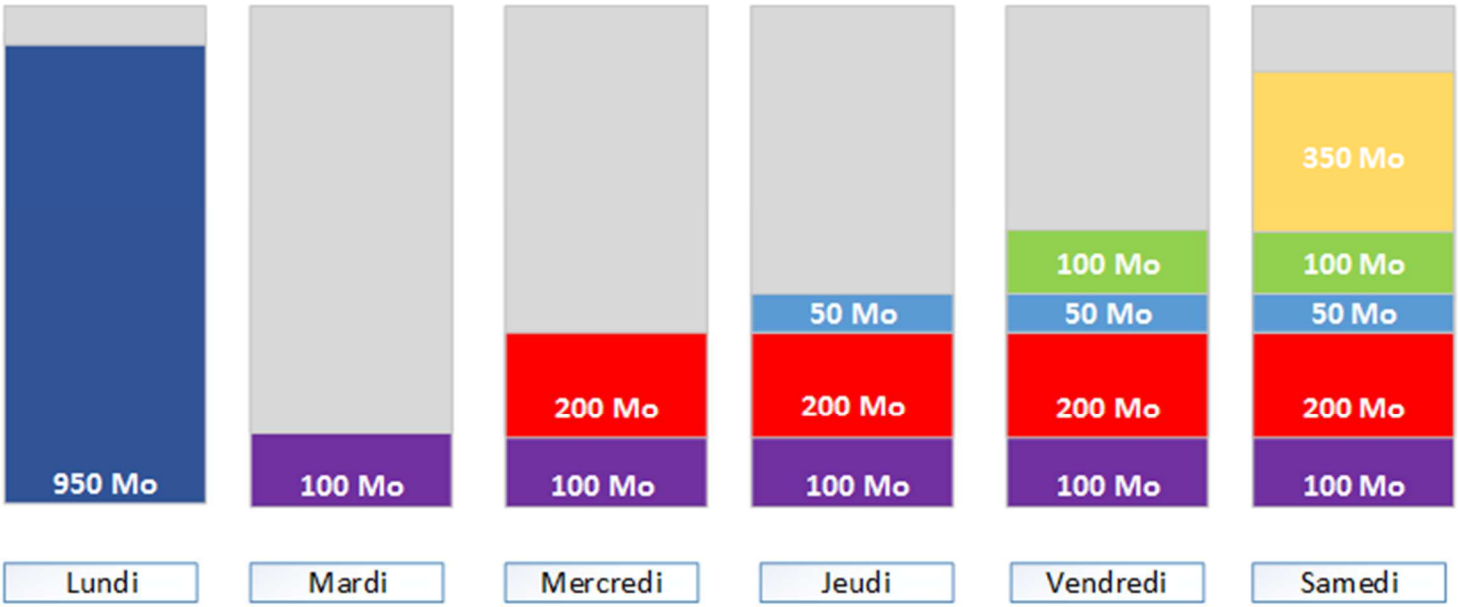
Mesure de sauvegarde

Pour anticiper la perte de données il faut mettre en place un plan de sauvegarde des données, trois types de sauvegarde sont possibles :

-La sauvegarde totale :

Une sauvegarde totale réalise une copie des données à sauvegarder sur un autre support

-La sauvegarde différentielle :



La sauvegarde différentielle s'occupe uniquement des fichiers modifiés depuis la dernière sauvegarde totale

Cette sauvegarde est plus lente et demande plus d'espace de stockage qu'une sauvegarde incrémentale mais elle est également plus fiable car seule la sauvegarde complète est nécessaire pour reconstituer les données sauvegardées.

Nous avons donc choisi de mettre en place un roulement avec treize supports de sauvegarde :

-Deux supports de sauvegarde totale (un support de sauvegarde par mois)

-Cinq supports de sauvegarde différentielles pour les mois paires (un support de sauvegarde par jour)

- Cinq supports de sauvegarde différentielles pour les mois impaires (un support de sauvegarde par jour)

-Un support de sauvegarde système totale (sauvegarde les fichiers système du serveur)

Anticiper le risque de divulgation des données

Les supports nomades doivent faire l'objet d'une sécurisation par chiffrement au vu de la sensibilité des dossiers ou documents qu'ils peuvent stocker. Le support de stockage des matériels informatiques obsolètes doit être physiquement détruits avant d'être jetés, ou en cas de don à des associations retiré le support de stockage avant. Les disques durs et les périphériques de stockage amovibles en réparation, réaffectés ou recyclés, doivent faire l'objet au préalable d'un formatage de bas niveau destiné à effacer les données qui peuvent y être stockées.

C. Intégrité des données

Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document accessible à l'ensemble des salariés. Sa rédaction nécessite l'inventaire préalable des éventuelles menaces et vulnérabilités qui pèsent sur le système d'information.

Il est important de faire évoluer régulièrement ce document, afin de suivre les modifications effectuées sur les systèmes et outils informatiques.

Sécuriser les postes de travail

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité. Les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Par ailleurs, le contrôle de l'usage des ports USB sur les postes « sensibles » est fortement recommandé.

Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures. Plusieurs types de protections seront mis en place au sein de l'entreprise :

- Des dispositifs de sécurité visant à protéger le réseau de l'entreprise,
- Une protection fiable contre les virus et logiciels espions tant sur le serveur que sur les postes des salariés,
- Une vigilance particulière concernant la messagerie électronique,
- La sécurisation des réseaux sans fil,
- Le contrôle des accès distants au système d'information par les postes nomades.

Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière via l'utilisation de badges d'accès.

Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

Le principal risque en matière de sécurité informatique est l'erreur humaine. Les utilisateurs du système d'information doivent donc être particulièrement sensibilisés aux risques informatiques via des formations, la diffusion de notes de service ou encore l'envoi périodique de fiches pratiques. Cette sensibilisation sera formalisée dans un document de type « charte informatique » afin de préciser les règles à respecter en matière de sécurité informatique, de messagerie électronique et d'Internet.

VI. Annexes

Table des annexes

Charte d'utilisation de l'outil informatique

Auto Concept

Cadre d'application

- L'entreprise met à votre disposition un outil informatique. Cet outil comprend un ordinateur, un accès à l'intranet, à Internet et des outils de communication. Le bon fonctionnement de ces éléments est régi par des règles simples mais strictes que chacun est tenu de respecter. Ces règles permettent l'intégrité et la sécurité des données de l'entreprise ainsi qu'une utilisation sans risques des outils.

- La présente charte définit donc les conditions d'utilisation des ressources informatiques en toute sécurité en rappelant à chacun ses obligations et ses devoirs.

Objet de la charte

I. Matériel mis à disposition :

- Chaque utilisateur doit prendre soin du matériel informatique mis à sa disposition (poste de travails, imprimantes …). L'utilisateur se doit de signaler le plus rapidement possible au service informatique tous disfonctionnements. Les interventions de dépannage et de maintenance seront uniquement réalisées par le service informatique.

II. Logiciels et fichiers personnels :

- L'installation de logiciels ne doit se faire que par le biais du service informatique. Chaque logiciel installé sur les postes informatiques sont autorisés dans l'entreprise qui détient pour ces logiciels les droits d'utilisation et les supports d'installation. La copie de ces logiciels est interdite quel qu'en soit l'usage sous réserve d'une autorisation explicitement signée par le directeur de l'entreprise.

- La demande d'achat d'un logiciel nécessite l'accord du directeur de l'entreprise avec la collaboration du service informatique. La demande d'installation d'un logiciel libre se fait directement au service informatique. La détention des supports est laissée à la charge du service informatique.

- L'utilisateur ne stocke sur son ordinateur ou sur les moyens de stockage mis à sa disposition que des fichiers ayant rapport avec son activité professionnelle, sous réserve d'une autorisation explicitement signée par le directeur de l'entreprise. L'utilisation et le stockage de certains fichiers sont répréhensibles pénalement (mp3, divx…) le stockage de ce genre de fichier sera sanctionné.

III. Sécurité des postes :

- Chaque poste informatique ou session est sécurisé par des mots de passes qui sont strictement personnels et ne doivent aucunement être divulgués à un tiers sauf au service informatique (cette mesure de sécurité est destinée à éviter les utilisations malveillantes ou abusives par un tiers).

- Le détenteur de la session mise en cause dans une utilisation illicite du poste sera considéré comme pénalement responsable de cette activité et sera sanctionné selon la gravité de ses actions.

IV. Réseau de l'entreprise :

En accédant aux ressources de l'entreprise l'utilisateur accepte les conditions suivantes :

- Il protège les informations et les données. Il est responsable des droits qu'il donne aux autres utilisateurs et il utilise les différents moyens de sauvegarde mis à sa disposition.
- Il n'utilise pas de comptes autres que le sien et ne masque pas sa véritable identité.
- Il ne tente pas de lire, de modifier, de copier ou de détruire des données autres que celles qui lui appartiennent.
- Il veille à verrouiller sa session avant de quitter, même provisoirement, son poste de travail.
- 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.

V. E-Mails :

L'utilisation de la messagerie électronique doit se faire avec certaines conditions. Les échange de mails doivent être cordiaux, sans propos préjudiciable.

Pour éviter les failles de sécurité ainsi que les virus, l'ouverture de pièces jointe se fait avec le maximum de précaution possible tout en vérifiant l'identité de l'expéditeur ; si celle-ci ne peut être vérifiée la pièce jointe ne doit pas être ouverte.

VI. Navigation Internet :

L'entreprise met à la disposition du salarié un accès à Internet dans un cadre professionnel durant les heures de travail. Durant les heures de pause il est permis de naviguer sur Internet librement dans le respect des lois.

L'utilisateur ne doit aucunement diffuser des informations de l'entreprise sur Internet.

VII. Contrôle des informations :

L'entreprise se réserve le droit d'accéder aux données sur un poste en présence de l'utilisateur concerné.

VIII. Sanctions applicables :

Le non-respect des règles relatées précédemment entrainera une sanction proportionnelle à la faute commise, les sanctions encourues peuvent être de nature disciplinaire, civile, administrative ou pénale.

Mise en application

Je soussigné(e)

Nom : ..... Prénom : .....

Service : ..... Fonction .....

Utilisateur des moyens informatiques et réseaux de la société AutoConcept déclare avoir pris connaissance de la présente charte et m'engage à la respecter.

Fait à..... Le .....

Signature du responsable Informatique :	**Signature de l'utilisateur :**

Charte Qualite Service Client

Chez PowerTech, la satisfaction client est une valeur fondamentale.
Voici les engagements que notre structure s'efforce de respecter au quotidien afin de garantir la satisfaction optimale de nos clients pour l'ensemble des services et prestations :

CONFIDENTIALITÉ :

PowerTech respecte et assure la confidentialité totale de toutes vos données numériques. Nos ingénieurs et techniciens sont de ce fait tenus au secret professionnel afin de ne divulguer aucune information vous concernant.

TRAÇABILITÉ :

PowerTech s'engage à vous informer par téléphone ou courrier électronique de l'évolution des dépannages informatiques que vous nous avez confié. Les demandes seront traitées et référencées en « Ticket » permettant une traçabilité dès votre appel jusqu'à la résolution finale du problème.

TRANSPARENCE :

PowerTech vous indique précisément la tarification avant intervention et détaille les actions qui seront entreprises. Nous vous fournissons un rapport détaillé pour chaque intervention effectuée. Le tarif est confirmé par devis ce qui vous garantit une intervention claire.

A L'ÉCOUTE :

PowerTech vous propose une qualité de conseil par des solutions adaptées à vos besoins. Nous nous engageons auprès de vous par une écoute attentive afin de répondre au mieux à vos attentes.

DISPONIBILITÉ :

PowerTech s'engage sur sa disponibilité tant en prise de rendez-vous qu'en intervention d'urgence et ce 6j/7. Cela se traduit par une réception rapide de vos appels et par la prise en charge directe de vos problèmes par un technicien qualifié.

CONTINUITÉ DE SERVICE :

PowerTech met en œuvre des solutions permettant de garantir la disponibilité maximale des équipements par une remise en service rapide en cas de panne. Cela est possible via une sauvegarde quotidienne de vos données ainsi que par la maintenance de vos équipements informatiques. Nous veillons à ce que votre système informatique soit parfaitement sécurisé et d'une utilisation aisée.

QUALITÉ DE SERVICE :

PowerTech vous garantit un accueil de qualité réalisé sur place ou au téléphone et la tenue ponctuelle de nos rendez-vous. Après chaque intervention, des enquêtes de satisfaction vous seront soumises dans l'objectif de nous améliorer sans cesse

Memo interne

Nos engagements :

- CONFIDENTIALITÉ
- TRAÇABILITÉ
- TRANSPARENCE
- A L'ÉCOUTE
- DISPONIBILITÉ
- CONTINUITÉ DE SERVICE
- QUALITÉ DE SERVICE

PowerTech

PowerTech
15 rue de la liberté, 21000 Dijon

PowerTech

Votre solution informatique

OBLIGATIONS SALARIÉS

Rapidité d'intervention

Tenue correcte

Hadopi

Haute Autorité pour la diffusion des œuvres et la protection des droits sur internet

Logiciels légaux

Confidentialité des données

Tests avant livraison

Explications claires

VII. Conclusion

Ce projet nous a permis d'acquérir des comportements appropriés en entreprise mais aussi de posséder les bases nécessaires à la gestion d'une entreprise en infogérance.

L'apport de solutions rapides à des problématiques par la création et le respect de nos engagements par l'intermédiaire d'une charte qualité.

VIII. Sources

[Abel Shakoo, « Comprendre la sauvegarde incrémentielle et différentielle »,site internet « IT-Connect » (25 Mar 2015) , http://www.it-connect.fr/comprendre-la-sauvegarde-incrementielle-et-differentielle/]

[CNIL , site internet CNIL (2017) https://www.cnil.fr/professionnel]

[Services publics, site internet du gouvernement (2017) https://www.service-public.fr/professionnels-entreprises/vosdroits/F24270]