CESi
ENSEIGNEMENT SUPÉRIEUR ET FORMATION PROFESSIONNELLE

PROJET SAS

M. Batiste BUFFAUT
M. Dylan DAUTEUR
M. Fabien DAUVERGNE
M. Jérémy DUPIN

13/12/2017

Table des matières

I. Présentation du projet SAS

Contexte :

Nous devons créer une entreprise fictive ayant pour principale activité la prestation informatique, qui a pour objectif d'obtenir la gestion du parc informatique (70 à 80 postes) du concessionnaire « AutoConcept ».

Plusieurs entreprises concurrentes ont aussi le même objectif.

Nous sommes chargés de réaliser une étude avant-vente.

Afin de réaliser ce projet, nous disposons des éléments suivants :

- Un cahier des charges
- Un compte-rendu du service commercial
- Des ressources extérieures (CNIL, Légifrance, Concept - ITIL)

Buffaut, Dauteur, Dauvergne, Dupin

II. Présentation de KeyServices

1. Présentation de l'entreprise

KeyServices est un prestataire de services informatiques situé au cœur de la ville de Dijon. Fondé en 2007 par Jean MILL, KeyServices assure l'organisation, le suivi et la mise en œuvre de toute l'infrastructure système et informatique.

KeyServices s'engage auprès de ses clients sur la qualité des prestations proposées en intégrant au sein de ses valeurs la volonté d'offrir aux entreprises un service personnalisé basé sur la disponibilité avec un délai rapide d'intervention, la compétence et la confiance. (cf. Annexe 1)

La société a toujours pu satisfaire, voire même anticiper les besoins des entreprises qui nous font confiance depuis plusieurs années.

KeyServices

10 rue de Lorraine
21000 DIJON
03 80 22 45 60

Ouverture de 8 h à 19 h du Lundi au Samedi

Téléphone : 03 80 22 45 60

Fax : 03 80 22 45 61

Mail : contact@keyservices.fr

Statut juridique : S.A.R.L. (Société à Responsabilité Limitée)

Capital : 13 600 €

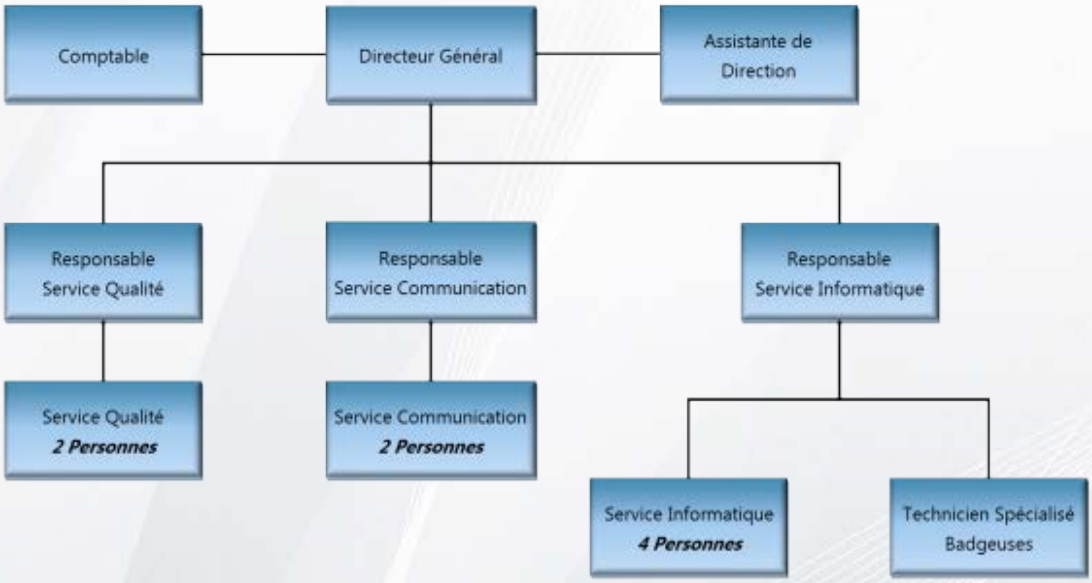
Responsable de l'entreprise : Mr Jean MILL

Activités : Installation et gestion de parcs informatiques pour professionnels sur le département de la Côte-d'Or (21).

Chiffre d'affaires (2016) : 946 000 €

Effectif : 15 personnes

2. Organigramme



Buffaut, Dauteur, Dauvergne, Dupin

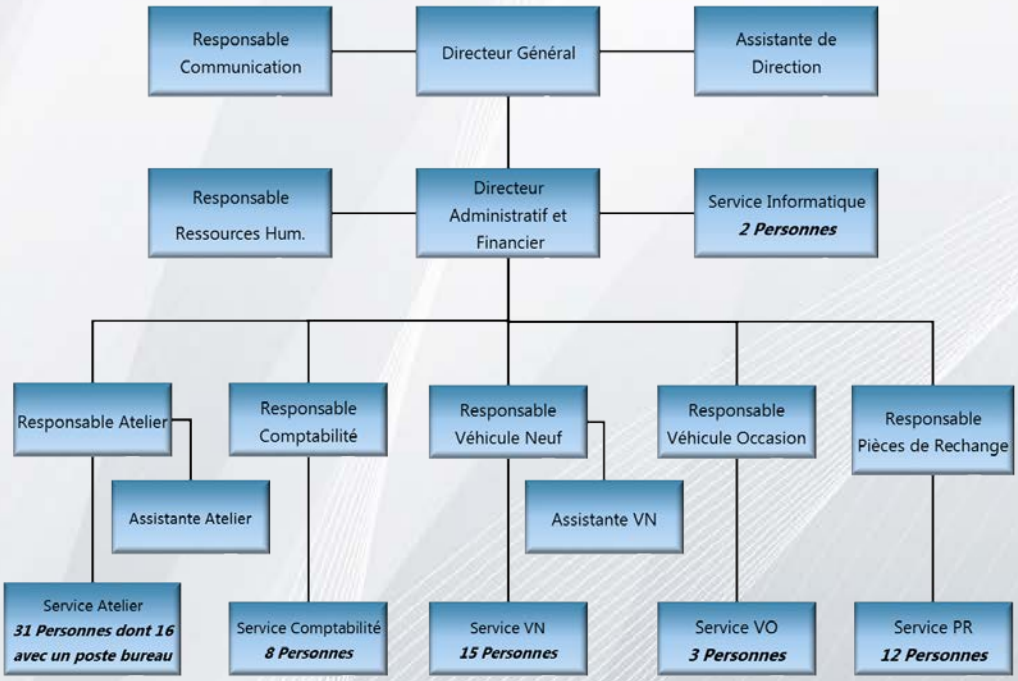
III. Présentation AutoConcept

1. Présentation de l'entreprise

AutoConcept est un concessionnaire automobile disposant actuellement d'un parc informatique de 80 postes. La société est actuellement à la recherche d'un prestataire pour externaliser leur maintenance informatique.

Afin de choisir au mieux son service, AutoConcept, qui a plusieurs entreprises en lice, souhaite avoir un maximum de sécurité ainsi que de la rapidité et de l'efficacité dans le travail de maintenance.

2. Organigramme



Buffaut, Dauteur, Dauvergne, Dupin

3. Problématiques

Actuellement, le parc informatique d'AutoConcept est géré par deux techniciens en interne. Suite à de nombreuses plaintes des utilisateurs, le concessionnaire souhaiterait se séparer de leurs techniciens. Pour se faire, AutoConcept propose à l'entreprise partenaire de recruter l'un des deux.

Les missions principales du prestataire de services sont :

- Administrer la maintenance du parc informatique
- Assurer un support utilisateur
- Supporter un moyen de solution pour la sauvegarde des données

IV. Synthèse sur l'utilisation de l'outil informatique en entreprise

1. Règles régissant l'utilisation des moyens informatiques mis à disposition des salariés

Contrôler l'utilisation d'Internet

Aujourd'hui, l'usage d'Internet au travail est indispensable pour les employés, c'est pour cela qu'il faut imposer des limites pour éviter tout débordement. Internet est utilisé à des fins professionnelles pour consulter des sites, télécharger des fichiers, participer à des forums de discussion ou échanger des courriers électroniques entre collègues ou avec une personne extérieure à l'entreprise.

Tout le monde utilise cet accès professionnel à des fins personnelles. La CNIL (Commission Nationale Informatique et Liberté) consent à dire qu'une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste. Elle préconise que les consultations à titre personnel ne dépassent pas un délai raisonnable et que les consultations ponctuelles de sites Internet ne concernent, sur le lieu de travail, que des sites dont le contenu n'est pas contraire à l'ordre public et aux bonnes mœurs (Rapp. CNIL, mars 2001 Rapp. CNIL, févr. 2002).

Contrôler les fichiers informatiques

Pour les juges, les consultations de sites Internet pendant le temps de travail et grâce à l'outil informatique mis à sa disposition par l'entreprise doivent avoir un caractère professionnel. Ce qui donne le droit à l'employeur de regarder les recherches de l'employé même en dehors de la présence du salarié (Cass. Soc., 9 juillet 2008, n° 06–45 800).

Cela autorise donc à inspecter le disque dur de l'ordinateur du salarié, à son insu, pour consulter la liste des téléchargements

Dans le même ordre d'idées, il est possible de consulter la liste des favoris de l'ordinateur professionnel du salarié sans l'en informer au préalable, l'inscription de sites Internet dans la liste des favoris de l'ordinateur professionnel du salarié ne leur conférant aucun caractère personnel (Cass. Soc., 9 février 2010, n° 08–45 253).

À noter : Lorsque l'entreprise met en place des logiciels permettant de surveiller les connexions des salariés (sites visités, temps passé, messages envoyés), ils doivent être déclarés à la CNIL et les salariés doivent en être informés.

Sanctions

Un usage abusif peut être sanctionné, seulement si l'employeur apporte la preuve de ce qu'il reproche à l'employé. Ce même abus peut être considéré comme une faute grave. (Cass. Soc., 18 mars 2009, n° 07–44 247) ;

Le salarié a le droit de consulter des sites pour des usages personnels, tant que le temps passé sur celui-ci reste raisonnable et légal.

Cependant si un employé se connecte à des sites à caractère pornographique, haineux ou à partager des informations qui peuvent faire courir un risque à l'image de la société, celui-ci commet une faute grave.

Fichiers stockés sur disque dur ou clé USB

Les fichiers créés par le salarié avec son accès sont présumés avoir un caractère professionnel et peuvent donc être ouverts par l'employeur.

Si les fichiers du salarié ont été identifiés comme personnel, l'employeur ne peut regarder ces fichiers que sous la surveillance de l'employé. (Cass. Soc., 18 octobre 2006, n° 04–48 025 et Cass. Soc., 18 octobre 2006, n° 04–47 400).

Buffaut, Dauteur, Dauvergne, Dupin

Si le salarié a identifié comme personnel des fichiers de son disque dur, l'employeur ne peut procéder à leur ouverture que s'il respecte deux conditions :

- Si le salarié est présent,
- S'il y a un risque particulier pour l'entreprise (Cass. Soc., 17 mai 2005, n° 03–40 017)

2. Charte informatique

Nous proposons à AutoConcept d'utiliser la charte informatique que nous avons rédigée. (cf. Annexe 2)

Posséder une charte informatique n'est pas obligatoire dans une entreprise, cependant elle est recommandée. Les avantages d'une charte informatique sont nombreux. Ce document permet au sein de l'entreprise de protéger légalement l'employé des utilisations des systèmes d'informations (Internet, téléphone, etc.) de ses employés. Cette charte réglemente l'utilisation des systèmes d'informations de l'entreprise permettant lors d'un usage contraire aux lois (tel qu'un téléchargement de données illégales) d'engager des poursuites pénales sur l'employé et non l'entreprise.

Une charte informatique doit être disponible à tout moment et doit être signée par les utilisateurs des systèmes d'informations, mais également à tous les futurs salariés de l'entreprise.

V. Plan de sécurisation des données

1. Politique de sécurité basée sur l'adoption du mot de passe

KeyServices a adopté une sécurité renforcée, non pas avec des mots de passe, mais avec un système de badges unitaires, spécifique à chaque salarié.

Ces derniers seront délivrés à chaque employé lors de leur arrivée au sein de l'entreprise et restitués au moment de leur départ.

Ce badge permet, à l'aide d'une badgeuse, la connexion du poste de travail et des comptes de l'employé et ainsi l'accès aux données. Cela est amené à sécuriser de manière optimale les systèmes de connexion. Le badge étant personnel, le risque d'échange ou de perte de mot de passe est exclu.

Ce système protège les données confidentielles à l'entreprise privant les utilisateurs de toute connexion extérieure.

2. Sensibilisation des utilisateurs à la nécessité d'adopter cette politique de sécurité

Les avantages de ce système sont les suivants :

1) Une sécurité optimale
2) Une confidentialité optimisée
3) Un risque moindre de piratage

3. Mesures de protection et de sauvegarde des données

Le système de sauvegarde est notre grande satisfaction. L'entreprise possède plusieurs modes de sauvegarde et de stockage. Comptant actuellement sur notre expertise pour ne perdre aucune donnée, une sauvegarde externalisée a été instaurée ainsi qu'un stockage directement sur serveur avec une sauvegarde hebdomadaire.

Stockage en ligne

L'ensemble des données sont sauvegardées sur le réseau, appelé « Cloud ». Il s'agit d'un stockage de données sur serveurs distants par l'intermédiaire d'un réseau Internet.

Stockage sur serveur physique

Un serveur physique récolte en temps réel l'ensemble des données qui seront ensuite répliquées et transférées directement sur le « Cloud ». Les données sur ce serveur sont sauvegardées la nuit de manière quotidienne afin de ne pas ralentir le bon fonctionnement du réseau.

L'atout de ces systèmes de stockage est d'exclure le risque de perte de données confidentielles en cas d'incident matériel et ainsi d'assurer la sauvegarde de l'intégralité des données.

Risques de dysfonctionnements

Afin d'anticiper tout dysfonctionnement électrique susceptible de survenir tel qu'une coupure de courant, des onduleurs seront déployés. Cet équipement permet de compenser une baisse de tension pouvant nuire à une perte d'exploitation.

4. Continuité des services en cas d'incident

Pour une prise en charge rapide et efficace, l'entreprise KeyServices dispose de 5 techniciens supervisés par un responsable informatique, répartis de la manière suivante :

- 4 techniciens informatiques
- 1 technicien spécialisé badgeuse

Les techniciens informatiques sont qualifiés afin d'intervenir rapidement et efficacement sur les incidents susceptibles de se produire. Cela garantit la rapidité de la prise en charge et ainsi de minimiser les pertes d'exploitations.

Intégré au sein de l'équipe informatique, le technicien spécialisé dans le système de sécurité assuré par les badges a pour mission principale de veiller au bon fonctionnement des badgeuses. La sécurisation d'accès reposant sur ce système, le délai d'intervention doit être rapide en cas de dysfonctionnement afin de préserver le travail des utilisateurs.

5. Support et accompagnement de qualité aux utilisateurs

KeyServices propose des formations aux utilisateurs afin d'empêcher divers dysfonctionnements :

- Problèmes liés à la sécurité
- Perte de temps et d'exploitation
- Propagation de virus

Grâce à ce dispositif, les utilisateurs sont sensibilisés à tous les dangers de la navigation et des virus perturbant le bon fonctionnement. Ces formations permettent également d'optimiser le temps de travail des salariés et d'enrichir leurs connaissances.

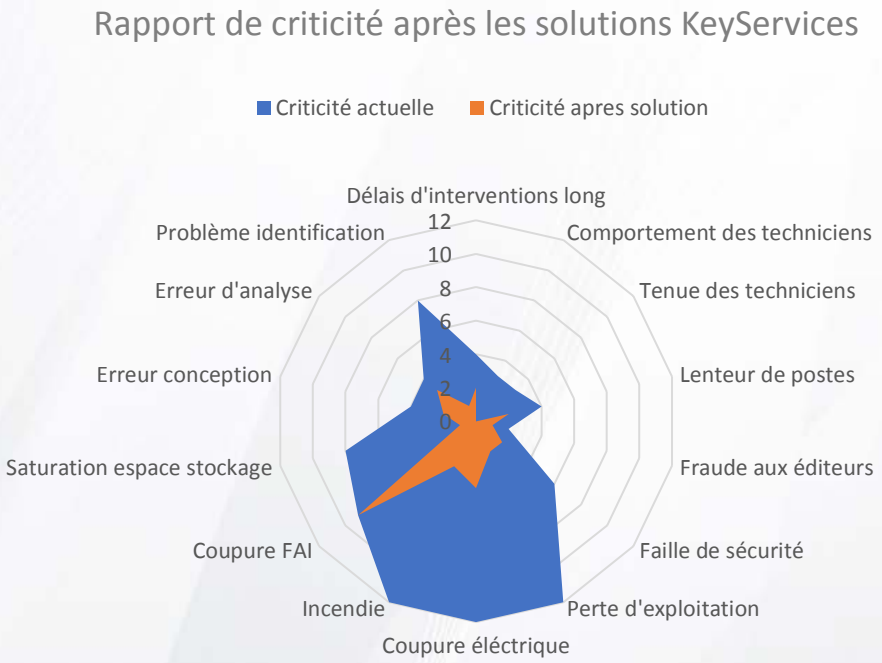
Chaque employé a la possibilité de suivre quatre heures de formation par mois. Deux sessions de formation sont organisées par mois permettant au salarié une plus grande flexibilité dans la prise de ces formations afin d'optimiser la participation de chacun.

Un tableau sera diffusé aux utilisateurs (cf. Annexe 3).

6. Sécurité et productivité du système d'information

L'efficacité, la fiabilité de la sécurité et de la productivité des systèmes d'informations sont les principales missions d'un service informatique. Une étude de risques courants dans une entreprise a été réalisée. Pour faire face à ces incidents, des solutions adaptées ont été proposées. Les résultats de cette étude sont exposés ci-dessous sous forme de graphique.

Cette analyse représente le taux de criticité des incidents qui étaient susceptibles de survenir avant l'étude de risques courants. Suite aux solutions préconisées par KeyServices, la criticité s'avère moindre en cas d'incident.



7. Mémo interne

Un mémo interne sera diffusé au sein de l'équipe du service informatique rappelant les valeurs de l'entreprise (cf. Annexe 4).

Une grande attention est portée notamment à la qualité des interventions ainsi que sur l'attitude à adopter face aux clients ou lors des appels téléphoniques.

8. Cas particulier : Recrutement d'un technicien d'AutoConcept

AutoConcept propose à l'entreprise KeyServices de recruter l'un des deux informaticiens actuellement présents dans la société.

Le recrutement se déroulera en deux étapes. Dans un premier temps, un test de positionnement permettra d'évaluer leurs compétences et leur savoir-faire. Dans un second temps, un entretien individuel aura lieu afin d'analyser leur savoir-être et ainsi de déterminer leurs motivations à rejoindre le service informatique de l'entreprise KeyServices.

À l'issue de cette sélection, le candidat se verra intégrer l'équipe et sera formé durant plusieurs semaines auprès d'un technicien informatique en vue de progresser sur ses qualifications et son professionnalisme.

De plus, le futur employé ne sera pas affecté aux missions concernant AutoConcept aux vues des circonstances évoquées.

VI. Conclusion

Le but de ce document est de montrer à la société AutoConcept que notre entreprise est la plus qualifiée pour prendre en charge leur parc informatique grâce aux moyens mis en place pour la sécurité des données ainsi que pour les modes de sauvegarde.

À travers ce document, nous avons exploré toutes les contraintes juridiques face aux utilisateurs, leur protection grâce à la charte informatique, ainsi que notre charte de qualité afin de montrer à AutoConcept notre éthique de travail.

KeyServices met tout en œuvre dans le but de satisfaire nos clients afin de répondre à leurs demandes spécifiques.

Avec les méthodes originales et développées que propose KeyServices, nous sommes confiants dans le fait que notre collaboration sera fructueuse.

Annexes

Annexe 1 : Charte qualité

Annexe 2 : Charte informatique

Introduction

L'entreprise AutoConcept met en œuvre des systèmes d'informations et de communications nécessaires à ses activités.

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 d'AutoConcept. L'entreprise met à disposition des utilisateurs : des ressources informatiques et communicatives.

La présente charte permet d'informer les utilisateurs sur le comportement à adopter vis-à-vis des moyens mis à disposition par AutoConcept. Cet outil permet aussi de sensibiliser les utilisateurs sur les risques dans l'utilisation des systèmes d'informations qui impliqueraient des conséquences graves pouvant engager la responsabilité civile ou pénale de celle-ci.

Domaine d'application

La présente charte s'applique à tout utilisateur du système d'information et de communication d'AutoConcept pour l'exercice de ses activités.

La charte est diffusée à l'ensemble des utilisateurs et remise systématiquement en main propre à tout nouvel arrivant et ainsi mise à leur disposition.

La charte s'applique sur tous les équipements informatiques (ordinateurs, serveurs, comptes en ligne, accès internet, etc.) possédés par AutoConcept.

Le non-respect des règles suivantes engage la responsabilité personnelle de l'utilisateur.

Règles d'utilisation

1. L'authentification

Des badges magnétiques **personnels** seront destinés à tous les utilisateurs après la signature de cette présente charte. Ces badges permettront aux utilisateurs d'avoir accès aux ressources nécessaires afin d'accomplir leurs différentes missions au sein de l'entreprise.

2. Règles de sécurité

Les utilisateurs s'engagent à respecter les règles suivantes.

En aucun cas, l'utilisateur ne doit :

- Usurper l'identité d'un autre utilisateur

- Utiliser un autre badge magnétique que celui qui lui a été remis.
- Installer, modifier ou supprimer un logiciel de l'entreprise

L'utilisateur est tenu de :

- Procéder à un verrouillage de son espace de travail en cas d'absence
- Signaler au responsable informatique les copies de données de l'entreprise sur un support externe
- Respecter l'intégrité physique et numérique de son matériel

3. Internet

Les utilisateurs doivent consulter uniquement les sites internet en rapport avec leurs activités professionnelles. Néanmoins, une utilisation ponctuelle et raisonnable d'un usage personnel de sites internet dont le contenu n'est pas contraire à la loi est tolérée.

À noter que l'historique des connexions sera archivé pour une durée de un an conformément au décret n° 2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne.

4. Messagerie électronique

L'entreprise AutoConcept met à disposition des adresses e-mail pour tous les utilisateurs.

Ces adresses e-mail sont uniquement destinées à un usage professionnel. Par conséquent, les usages personnels, commerciaux, ou tout autre usage extérieur au domaine d'application sont interdits.

5. Administrateur des systèmes informatiques

Les administrateurs des systèmes informatiques peuvent être amenés à examiner le contenu de fichiers ou e-mails afin de vérifier en cas de doute, le respect de cette présente charte.

De plus, les administrateurs s'engagent à préserver la confidentialité des données personnelles sur lesquelles ils seront confrontés.

6. Accès internet et pare-feu

Un accès internet est disponible après l'authentification de l'utilisateur sur sa session personnelle. Néanmoins, un système de filtrage et de surveillance est activé afin de protéger les utilisateurs.

L'accès internet est filtré de manière suivante :

- Blocage des sites pouvant être nuisibles à l'entreprise (sites pornographiques, pédophiles, incitant à la haine, téléchargement illégal, etc.)

- Limitation et surveillance du temps de présence sur les sites consultés à des fins personnelles

Procédure de départ

En cas de départ de l'entreprise AutoConcept, l'utilisateur est tenu de **:**

- Supprimer toutes les données personnelles en rapport avec lui-même et l'entreprise
- Faire une demande d'autorisation au chef de service pour garder toutes copies de documents professionnels
- Procéder à une remise de son badge magnétique

Les comptes de l'utilisateur seront supprimés dans un délai maximum d'un mois.

Sanctions

Les utilisateurs ne respectant pas cette présente charte peuvent, après consultation des supérieurs hiérarchiques, être exposés aux sanctions suivantes selon la gravité de la violation de cette charte :

- Avertissement
- Pare-feu plus strict (restriction de l'accès internet)
- Poursuites judiciaires

Le non-respect des lois et textes applicables en matière de sécurité des systèmes d'informations est susceptible de sanctions pénales prévues par la loi.

Durée de validité

L'entreprise AutoConcept se réserve le droit de changer cette présente charte comme elle le souhaite à tout moment. Cette charte est valide dès lors de la signature de l'utilisateur et pour une durée de un an. Le contrat doit donc être renouvelé chaque année.

DISPOSITIONS LÉGALES 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 modifiées par la loi n° 2004-801 du 6 août 2004. Dispositions pénales : – Code pénal (partie législative) : art 226-16 à 226-24 — Code pénal (partie réglementaire) : art R. 625-10 à R. 625-13

Loi n° 88-19 du 5 janvier 1988 relative à la fraude informatique dite loi Godfrain. Dispositions pénales : art 323-1 à 323-3 du Code pénal. 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. Disposition pénale : art L.335-2 du Code pénal

---

Je soussigné(e) : ……,

M'engage à respecter cette présente charte

Fait le ……., à ……,

Signature précédée de la mention « Lu et approuvé »

Annexe 3 : Tableau de formation

Formation informatique AutoConcept

Thème de la formation :

Proposition n° 1 Date — Heure Durée (4 h)		**Proposition n° 2 Date — Heure Durée (4 h)**	
Nom — prénom	Signature	Nom — prénom	Signature

Buffaut, Dauteur, Dauvergne, Dupin

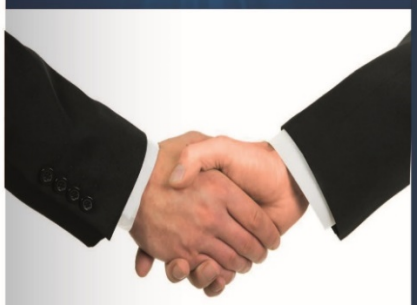
Annexe 4 : Mémo interne

CONFIDENTIALITÉ

Les données « utilisateurs clients » sont **strictement confidentielles**.

Ces informations privées ne doivent en aucun cas être divulguées.

management compétences manager groupe efficacité travail d'équipe professionnel compétitivité motivation projets ÉQUIPE personnel collaboration esprit d'équipe réunion gestion entreprise ressources humaines co-opération ensemble performance



contact@keyservices.fr
03 80 22 45 60
www.keyservices.fr

MÉMO INTERNE

key services
La clé de votre succès

Attitude face aux clients

Ponctualité : respect des horaires lors des rendez-vous clientèle et des délais d'intervention

Politesse : emploi d'un langage approprié pour chaque interlocuteur

Disponibilité : utilisation de phrases affirmatives pour rassurer les utilisateurs

Pédagogie : explication de manière concrète des solutions apportées

Professionnalisme : choix d'une tenue vestimentaire propre et correcte

Attitude au téléphone

- Enoncer le nom de l'entreprise, se présenter et adresser un « bonjour » enthousiaste
- Ecouter attentivement l'utilisateur afin d'analyser le dysfonctionnement
- Parler clairement, distinctement et adopter une attitude positive face à l'interlocuteur
- Créer un ticket incident (GLPI) pour la traçabilité de l'intervention permettant d'assurer un suivi optimal

Attitude en intervention

- Envoyer par mail le suivi de l'intervention à l'utilisateur fixant les délais
- Utiliser des logiciels professionnels avec licences
- Tester le matériel avant la restitution au client
- Informer immédiatement votre supérieur en cas de découverte de données illégales