



RÉPONSE À L'APPEL D'OFFRES

Pour l'entreprise
AutoConcept

PROJET SAS DE :

**GUINOT ROMAIN
ROCHE DYLAN
VERDIER ANTOINE
VILLALOBO OLIVIER**

SOMMAIRE

1. PRÉSENTATION DE IT SOLUTION	2
1.1 Informations légales	3
1.2 Organigramme IT SOLUTION	3
1.3 Localisation et plan de l'entreprise	4
1.4 Informations générales	5
2. PRÉSENTATION DU CLIENT	6
2.1 Informations légales	7
2.2 Organigramme de la société AutoConcept	7
2.3 Localisation et plans de l'entreprise	8
3. RÈGLES D'UTILISATION DE L'INFORMATIQUE EN ENTREPRISE	9
Charte informatique	9
Stockage et utilisation des données	9
Les mots de passes	10
Solutions de filtrage	10
4. PLAN DE SÉCURISATION DES DONNÉES	11
Stratégie des mots de passes	11
Sécurisation de l'accès aux données	12
Sécurisation des données	12
5. PLAN DE MISE EN CONFORMITÉ	13
6. ANNEXES	14
6.1 Charte Informatique	14
6.2 Charte qualité service client	18
6.3 Mémo interne	19
6.4 Contrat Infogérance	20
6.5 Devis	24
6.6 Sources	25
6.7 Glossaire	25

1. PRÉSENTATION DE IT SOLUTION



TEL : 05 56 54 34 67 – 07 60 57 17 72

Adresse: 21 Allée de Chaminaux 33000 Bordeaux

Directeur: WILLIS Rodrigue

Statut social: SARL

Certifié ISO 20000-1

Mail: it.solution@gmail.com

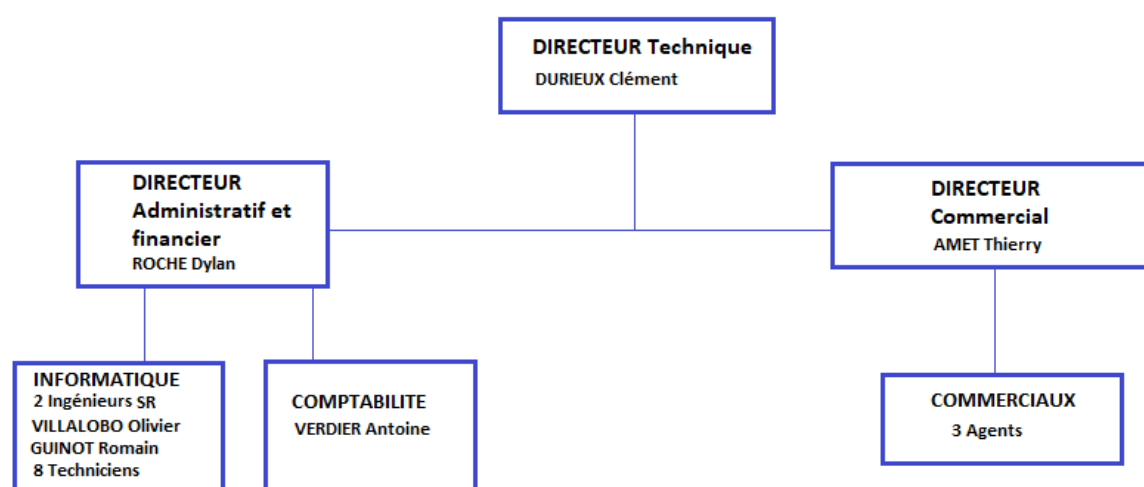


IT SOLUTION a été créée au début des années 1990 par un ingénieur informaticien français du nom de WILLIS Rodrigue à Bordeaux. Elle est spécialisée dans l'infogérance, la vente et l'installation de matériel informatique pour des professionnels et des particuliers.

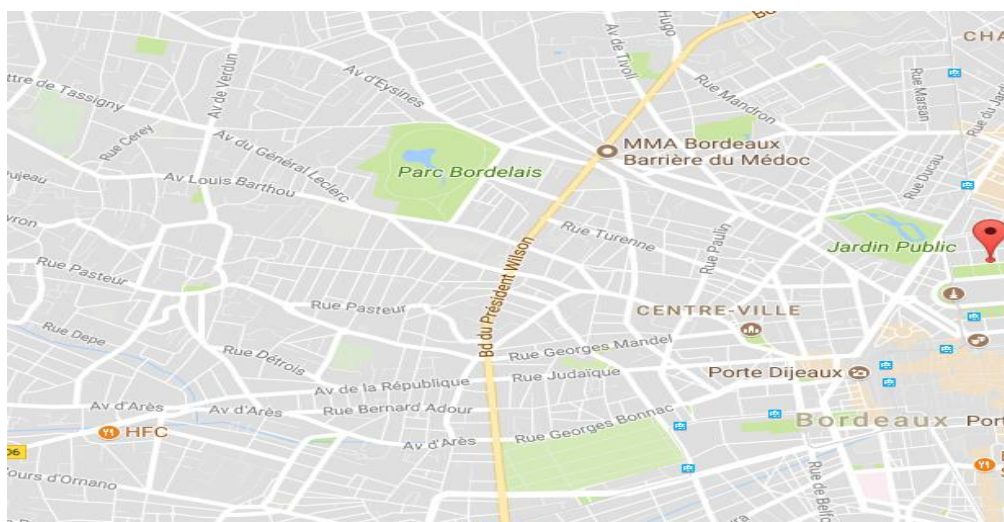
1.1 Informations légales

Dénomination	IT SOLUTION
Adresse	21 Allée de Chaminaux 33000 Bordeaux
Téléphone	05 56 54 34 67 – 07 60 57 17 72
SIREN	344 049 580
SIRET (siège)	34404958000030
Forme juridique	SARL
Date immatriculation RCS	18-03-1992
Tranche d'effectif	15 à 30 salariés
Capital social	185 000,00 €
Chiffre d'affaires 2016	1 102 000,00 €

1.2 Organigramme IT SOLUTION



1.3 Localisation et plan de l'entreprise



1.4 Informations générales

Activités

- Infogérance (Certifié ISO 20000-1)
- Installation de postes et de leurs différents périphériques
- Dépannage hardware / software
- Maintenance serveur / installation / sécurité réseaux et données

Partenaires

- CESI
- TBM
- TOYOTA
- CYBERTEK
- CISCO
- APPLE

Clients

- Cabinets médicaux
- Mairie de Bordeaux
- Centre de formation

2. PRÉSENTATION DU CLIENT



AutoConcept est un garage automobile disposant d'un parc informatique de 70 postes. Suite à quelques problèmes avec son service informatique, AutoConcept souhaite sous-traiter la maintenance de son parc informatique et ainsi solliciter un prestataire. L'entreprise engagée devra fournir une solution de sauvegarde des données et assurer la maintenance du parc informatique ainsi que le support de ses utilisateurs.

AutoConcept a été créée en 2000 par un français du nom de AMOLO Philippe à Bordeaux. Elle répare et vend des véhicules pour des professionnels et des particuliers.

AutoConcept

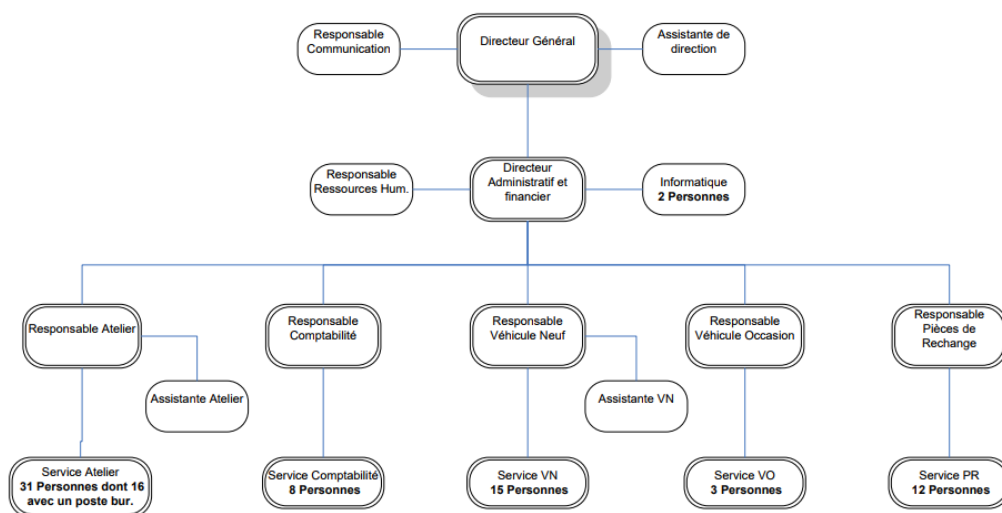
3 Rue du Colisée, 33000 Bordeaux

06 67 45 24– 07 67 56 78 79

2.1 Informations légales

Dénomination	AutoConcept
Adresse	3 Rue du Colisée, 33000 Bordeaux
Téléphone	05 56 67 45 24- 07 67 56 78 79
SIREN	644 449 522
SIRET (siège)	3304958000060
Forme juridique	SARL
Date immatriculation RCS	18-03-2000
Tranche d'effectif	50 à 100 salariés
Capital social	1 785 000,00 €
Chiffre d'affaires 2016	4 589 600,00 €

2.2 Organigramme de la société AutoConcept



2.3 Localisation et plans de l'entreprise



3. RÈGLES D'UTILISATION DE L'INFORMATIQUE EN ENTREPRISE

Dans le cadre du compte-rendu qui nous a été remis, de nombreuses fautes professionnelles ont été rapportées. Certaines d'entre elles peuvent justifier d'une sanction pénale, c'est pourquoi nous avons jugé nécessaire de rappeler le cadre légal qui entoure l'utilisation de l'outil informatique en entreprise :

Charte informatique

En annexe de ce dossier se trouve une charte informatique regroupant les cadres et utilisations des outils informatiques. Cette charte est à destination de tous les employés d'AutoConcept et leur est opposable. Cette charte sera à signer et à inclure au contrat de travail pour les futurs recrutements au sein de l'entreprise et aura un effet rétroactif pour les salariés actuels.

La charte informatique est tout autant un outil clarifiant le cadre légal de l'utilisation du système d'information qu'un outil de communication. Au travers cette charte, il est porté à la connaissance de l'employé tout ce qui lui est autorisé, restreint et interdit.

Stockage et utilisation des données

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur ne peut pas librement consulter les courriels personnels de ses employés ni, sous certaines conditions, avoir accès à leurs données privées stockées sur le réseau et ce même si l'employeur a interdit d'utiliser les outils de l'entreprise à des fins personnelles. Pour qu'ils soient protégés, les messages et les dossiers personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé »

Les articles 226-15, alinéa 2 du code pénal concernant le secret de la correspondance privée et l'article 226-18 du code pénal interdisent de recueillir des informations privées sans consentement de l'utilisateur.

En revanche, dans le cadre d'une procédure judiciaire, un huissier peut parfaitement être mandaté par le tribunal pour consulter et prendre copie des messages personnels du salarié dans la mesure où ces éléments d'information peuvent éclairer les décisions des juges, par exemple pour vérifier les actes de concurrence déloyale dont le salarié est accusé (Cour de cassation, arrêt du 10 juin 2008).

Les mots de passes

Il n'y a aucune loi encadrant la création des mots de passe, uniquement des recommandations comme celles de la CNIL (cf. annexe).

Cependant, des lois encadrent et définissent la "valeur" des mots de passes en entreprise. Un mot de passe protège un espace de travail possédant lui-même des espaces personnels comme des dossiers "Privé" par exemple. Ce qui est la raison pour laquelle être en possession du mot de passe d'un collègue et utiliser son compte, en se faisant passer pour lui ou non, constitue une infraction pénale.

L'article 226-4-1 du code pénal réprime le délit d'usurpation d'identité en sanctionnant d'un an de prison et de 15 000 euros d'amende

Solutions de filtrage

En entreprise les connexions internet sont supposées avoir un caractère professionnel.

L'employeur a donc le droit de consulter et vérifier les sites visités par le salarié en dehors de sa présence et sans son accord. Au sein d'AutoConcept, le pare-feu et le proxy serviront au filtrage et à la protection des données de l'entreprise. Avec ces derniers, un suivi de connexion aux sites web est possible. L'employeur pourra donc sanctionner le salarié si d'éventuels abus sont constatés. À condition de pouvoir prouver que ces connexions établies pendant les horaires de travail sont bien le fait du salarié concerné.

Arrêt du 9 juillet 2008, n°06-45.800 de la cour de cassation.

4. PLAN DE SÉCURISATION DES DONNÉES

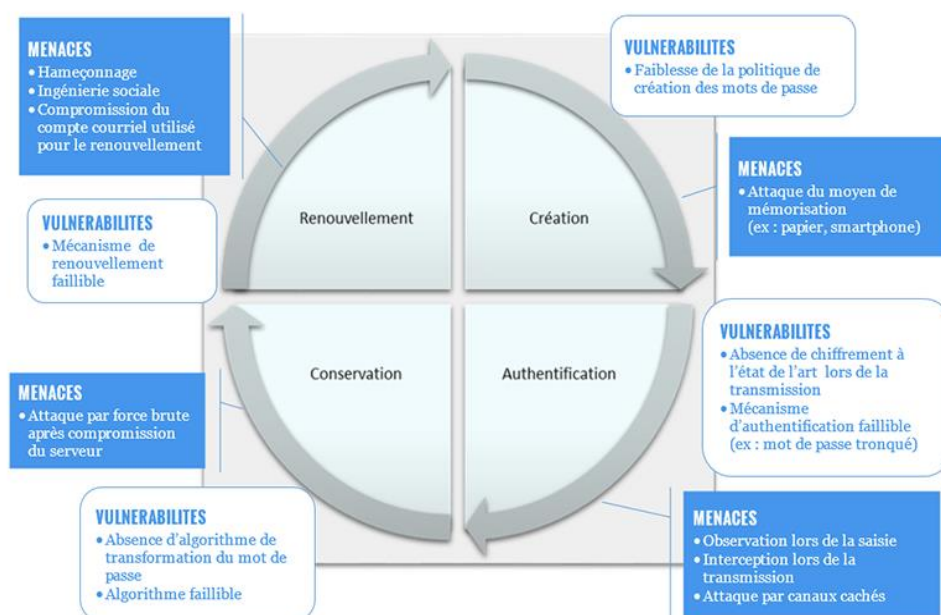
Dans le cadre de notre intervention chez AutoConcept, nous proposons un plan de sécurisation des données en plusieurs étapes :

Stratégie des mots de passes

Première pierre de l'édifice sécuritaire d'un système d'information, la stratégie des mots de passes est essentielle et bien souvent négligée. Sécuriser son système d'information passe obligatoirement par cette étape, ce qui explique les mesures de sécurité suivantes :

- 8 caractères minimum, dont au moins une majuscule.
- Ne doit contenir ni le nom ni le prénom de l'utilisateur
- Les mots de passe seront changés tous les 6 mois. Un e-mail sera envoyé une semaine avant le changement, puis la veille et finalement le matin même. Il sera demandé aux utilisateurs de se déconnecter de leur session avant de partir déjeuner pour que le changement puisse être effectué à 13h.
- Les mots de passe sont strictement personnels et confidentiels, en aucun cas ils ne peuvent être partagés ni écrits sur un document.
- Le service informatique ne connaîtra pas votre mot de passe et en aucun cas sera amené à vous le demander. Ne le partagez pas.

Chaque employé est responsable de son mot de passe et donc de la sécurité des données de l'entreprise. L'image suivante permet de bien comprendre l'intérêt d'une politique de mots de passes forte et réfléchie :



Sécurisation de l'accès aux données

Notre objectif est de réunir tous les ordinateurs du parc dans un seul domaine et de centraliser le tout avec un contrôleur de domaine. Des groupes d'utilisateurs seront définis via l'Active Directory afin de faciliter la distribution et le contrôle des droits d'accès aux différents dossiers et sous dossiers.

Sécurisation des données

Pour assurer la sécurité des données, nous préconisons d'agir sur deux axes :

Au niveau logiciel :

- MCAFEE, qui est l'antivirus actuel d'AutoConcept, sera réinstallé sur tous les nouveaux postes et serveurs du parc informatique.
- Un proxy sera également présent pour filtrer le contenu venant de l'extérieur avant qu'il ne pénètre sur le réseau (cf. charte informatique en annexe).
- Un VPN sera installé sur les ordinateurs portables des commerciaux pour qu'ils puissent à distance se connecter sur le réseau local de l'entreprise.

Au niveau physique :

- Une salle homologuée (dépollution de la salle, climatisation efficace pour le contrôle de température, du matériel de détection d'incendie, un extincteur et un contrôle d'accès) sera préparée pour recevoir le nouveau serveur qui servira pour l'ERP, les sauvegardes et les mises à jour. La manière dont nous proposons de gérer le système d'information nécessite un serveur avec plus de puissance que ce que leur serveur peut offrir pour le moment. Ce coup supplémentaire est réfléchi, nous le jugeons indispensable pour l'avenir.
- En plus des techniciens de IT SOLUTION, seul le directeur du garage possèdera les clés de la salle informatique.
- Les données de l'entreprise seront sauvegardées à l'aide d'une sauvegarde complète puis différentielle. Chaque dimanche soir, une sauvegarde complète sera effectuée et chaque soir de la semaine une sauvegarde différentielle permettra de sauvegarder uniquement les fichiers modifiés jusqu'à la sauvegarde complète suivante. Le logiciel utilisé sera Handy Backup. Ce système de sauvegarde est entièrement fiable puisqu'il suffit que de la sauvegarde complète pour restaurer les données. De plus, nous préconisons l'utilisation du RAID5 pour stocker les fichiers sauvegardés avec les sauvegardes différentielles.

Nous avons opté pour cette solution, coûteuse en espace de stockage mais fiable, pour ne plus être confronté aux problèmes de perte de données qu'AutoConcept a déjà connu. Un pare-feu sera installé et des politiques de filtrage seront définies pour garantir l'intégrité et la sécurité des données.

5. PLAN DE MISE EN CONFORMITÉ

Dans le cadre de la mise en conformité et d'harmonisation du parc informatique, nous préconisons le renouvellement de tous les postes. Pour se faire, nous proposons de lisser ce renouvellement sur 12 mois.

Il faudra changer les 50 postes sur Windows XP en premier lieu, puis sur les 12 mois suivants, prévoir le renouvellement des 20 ordinateurs restants. Le parc actuel consiste en 66 ordinateurs fixes et de 4 ordinateurs portables, donc pour le moins possible perturber l'utilisateur, nous préconisons de garder ce ratio. L'ancien bureau des deux informaticiens servira d'atelier et de salle pour entreposer le matériel de rechange : 2 ordinateurs fixes, 2 ordinateurs portables et des périphériques. Les nouveaux ordinateurs seront tous fournis avec des licences office 365 ainsi que Windows 7 Pro afin de palier au problème d'utilisation de licences non officielles, ce qui, pour rappel, est illégal.

Un nouvel onduleur sera fourni pour remplacer le modèle équipant actuellement AutoConcept, fournissant assez de courant pour permettre de sauvegarder et d'éteindre en toute sécurité le serveur, le modèle actuel ne pouvant plus remplir ce rôle.

Le technicien recruté par IT SOLUTION sera formé à nos techniques les 3 premiers mois puis, par la suite, intégrera notre équipe de technicien volant. Il sera amené à intervenir auprès de son ancienne société AutoConcept mais ne sera pas prioritaire sur ses collègues.

6. ANNEXES

6.1 Charte Informatique

Préambule

La charte a pour objet de définir les modalités et les conditions d'utilisation des moyens informatiques de la société AUTOCONCEPT et d'Internet.

Il s'agit d'un code de déontologie qui a pour objectif d'informer, de sensibiliser chaque utilisateur en proposant des règles d'utilisation, et de préciser la responsabilité en matière de droits et d'obligations de chacun. La transgression des règles de bonne conduite qui s'imposent peut conduire l'utilisateur à engager sa responsabilité civile ou pénale, ainsi que celle de la société.

La présente charte ne vise pas à être exhaustive en termes de droits qui doivent être respectés : elle contient les règles et obligations essentielles que l'utilisateur ne doit pas méconnaître et respecter au profit d'autrui et de l'entreprise sans préjudice du respect des autres lois, textes ou usage en vigueur.

Ce document est vivant : il est susceptible d'être modifié en fonction de l'évolution de la jurisprudence, de la législation, de la technologie et du système d'information de la société AutoConcept

Accès aux ressources informatiques

L'utilisation des ressources informatiques de l'entreprise AutoConcept, l'usage des services Internet ainsi que du réseau pour y accéder sont limités au cadre exclusif de l'activité professionnelle, conformément à la législation en vigueur et aux règles de tolérance concernant la correspondance privée. Ainsi toute information est considérée comme professionnelle à l'exclusion des données explicitement désignées par l'utilisateur comme relevant de sa vie privée. Il appartient donc à l'utilisateur de procéder au stockage éventuel de ses données à caractère privé dans des répertoires explicitement prévus à cet effet et intitulés « privé ».

L'utilisation des périphériques de stockage externes (disques durs, clés USB, ...) est soumise aux règles qui contribuent au maintien de la protection de l'information. Les raccordements des ressources informatiques ne pourront pas être modifiés sans autorisation préalable. De même toute modification des configurations logicielles des matériels mis à disposition par la société AutoConcept est interdite.

Les utilisateurs disposent d'un compte individuel auquel ils accèdent en saisissant leur nom d'utilisateur (identification) et un mot de passe (authentification) qu'ils choisissent eux-mêmes.

Le droit d'accès aux ressources informatiques de la société est personnel, incessible et temporaire et peut être retiré à tout moment. Il disparaît notamment dès que son utilisateur ne remplit plus les conditions qui lui ont autorisé l'accès, notamment en cas de départ de la société AutoConcept. Il peut être retiré en cas de non-respect de la présente charte.

Déontologie informatique

Chaque utilisateur, qui est juridiquement responsable de l'usage qu'il fait des ressources informatiques, s'engage à respecter les règles de déontologie informatique et notamment à ne pas effectuer intentionnellement des opérations qui pourraient avoir des conséquences néfastes sur le fonctionnement du réseau, ou sur l'intégrité de l'outil informatique.

En particulier, il doit se garder :

- de masquer sa véritable identité,
- de s'approprier le mot de passe d'un autre utilisateur,
- de diffuser son mot de passe,
- de modifier, d'altérer ou de détruire des informations ne lui appartenant pas sur un des systèmes informatiques connectés au réseau d'AutoConcept
- de développer des outils mettant sciemment en cause l'intégrité des systèmes,
- de contourner les moyens de protection mis en place
- d'accéder à des informations appartenant à d'autres utilisateurs sans leur autorisation, notamment le courrier électronique,
- d'interrompre le fonctionnement normal du réseau ou d'un des systèmes connectés ou non au réseau (éteindre un serveur, déconnecter un câble réseau, introduire un virus...)

Toute négligence grave ou répétée est considérée comme fautive et peut entraîner des mesures disciplinaires et la fermeture immédiate des droits d'accès.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation, le détournement à des fins personnelles et la nécessité de mettre en œuvre des moyens humains ou techniques supplémentaires pour en contrôler l'usage

L'utilisateur a la charge, à son niveau, de contribuer à la sécurité générale. En particulier, il doit :

- assurer la protection de ses informations ; il est responsable des droits qu'il donne aux autres utilisateurs ; il lui appartient de protéger ses données en utilisant les moyens de sauvegarde mis à sa disposition,

- signaler toute tentative de violation de son compte, et, d'une manière plus générale, toute anomalie constatée
- ne pas permettre à des personnes non autorisées par la société AutoConcept l'usage ou l'accès à des données, des systèmes et des réseaux, soit à travers le matériel dont il a l'usage, soit par transfert volontaire de données par quelque moyen que ce soit (Internet, disquettes, CD, clés USB, ...),
- choisir des mots de passe sûrs, les changer régulièrement, et veiller à leur secret,
- ne pas quitter son poste de travail ou un poste partagé sans se déconnecter ou sans verrouiller sa session,

De façon particulière, les utilisateurs ne doivent en aucun cas effectuer d'expérimentation sur la sécurité des systèmes et réseaux informatiques ou sur les virus informatiques. Le développement, l'usage et la simple détention de logiciels ou programmes visant à contourner la sécurité des systèmes ou la protection des logiciels, sont strictement prohibés et illégaux.

Règles

Il est interdit de réaliser des copies de logiciels commerciaux pour quelque usage que ce soit. L'utilisateur ne doit pas installer de logiciels lui-même, y compris ludiques, ni contourner les restrictions d'utilisation d'un logiciel.

Il est interdit de télécharger des vidéos, photographies, images, fichiers sonores ou autres créations protégées par le droit d'auteur ou un droit privatif sans avoir au préalable obtenu l'accord du titulaire de ces droits. Il est interdit de stocker des vidéos, photographies, images, fichiers sonores ou autres créations protégées par le droit d'auteur ou un droit privatif sur les postes de travail ou les serveurs, le groupe hospitalier ne pouvant prouver que l'accord du titulaire des droits a été obtenu.

Usage des services Internet : L'utilisateur doit faire usage des services Internet dans le cadre de ses activités professionnelles et dans le respect des principes généraux et des règles propres aux sites consultés ainsi que dans le respect de la législation en vigueur.

La consultation de sa ou ses messageries personnelles et de sites sur Internet est tolérée, en dehors du temps de travail, pour des motifs non professionnels légitimes à partir d'un poste de travail mis à sa disposition par la société AutoConcept dans le strict respect des règles énoncées dans cette charte.

Filtrage réseau : Un proxy et un pare-feu sont mis en place afin de filtrer les données entrantes et sortantes du réseau. Conformément à la loi du 21 juin 2004, dite

LCEN, article 6 II, les historiques de navigation ainsi que les identifiants de connexion sont gardés pendant un an et sont à la disposition des forces de l'ordre.

Tout utilisateur de l'Internet ne doit pas :

- harceler par e-mail (envoi de messages abusifs, pourriels (spams)...) un individu à l'aide des outils informatiques,
- se connecter ou essayer de se connecter sur un site sans y être autorisé (tentatives de piratage, usurpation d'identité, usage de comptes / mots de passes volés ou à l'insu de leur propriétaire, ...),

Le non-respect par l'utilisateur de ces principes pourra entraîner des sanctions disciplinaires, lesquelles peuvent aller jusqu'au licenciement pour faute grave.

Exemples de risques

La transmission d'informations nominatives ou la divulgation d'autres informations sensibles en clair par messagerie sont des atteintes à la confidentialité qui engagent la responsabilité de l'utilisateur responsable et de l'entreprise pour défaut de sécurité. Le téléchargement par le web de logiciels douteux peut rendre possible l'intrusion de virus informatique et la divulgation d'informations. Un mot de passe laissé en clair à côté d'un poste de travail peut être la porte ouverte à une introduction frauduleuse dans notre système d'information

En cas de manquements à cette charte

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à un licenciement ainsi qu'à des sanctions et poursuites pénales prévues par les textes législatifs et réglementaires en vigueur.

- Loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés».
- Lois sur la fraude informatique, article 323-1 à 323-7 du code pénal.

La présente charte est applicable à compter du : 13/10/2017

(Elle a été adoptée après information et consultation du comité d'entreprise OU des délégués du personnel et du comité d'hygiène et de sécurité en date du 01/10/2017)

Signatures :

AutoConcept

Service informatique



6.2 Charte qualité service client

Afin de vous satisfaire au mieux, IT SOLUTION s'engage sur plusieurs points :

ACCUEIL

Vous offrir un accueil personnalisé, impliqué, dynamique et respectueux.

ÉCOUTE DES ATTENTES

Travailler à vos côtés où l'écoute et la compréhension de vos besoins et attentes seront le socle de tous nos projets.

RIGUEUR ET CONSEILS

Tout mettre en œuvre pour satisfaire vos attentes dans les meilleurs délais en vous proposant les solutions les plus adaptées. Chaque proposition vous sera présentée en détails et nécessitera votre validation avant implémentation.

DISPONIBILITÉ

Tout au long de l'année nous intervenons entre 8h et 19h du lundi au vendredi. Des interventions hors jours ouvrés sont possibles en fonction de la gravité de la panne.

TRANSPARENCE

Vous fournir une tarification claire ainsi que le détail de chaque intervention. Vous ne serez jamais laissé dans l'inconnu : la transparence est le nerf de la confiance.

ENGAGEMENT SUR LA DURÉE

Tout au long de l'année : s'assurer de votre satisfaction et faire un suivi des garanties matériel et logicielles (cf contrat d'infogérance en annexe)

CONTINUITÉ DU SERVICE

Nous intervenons en moins d'une heure et rétablissons vos services en moins de 24h en cas de panne. Nous mettons à votre disposition toute la documentation relative à vos installations en plus de procédures compréhensibles par tous.

6.3 Mémo interne

Cette note est à destination des techniciens de IT SOLUTION.

Tenue vestimentaire

La tenue vestimentaire est un élément majeur lors d'une intervention chez un client, celle-ci reflète l'image de l'entreprise, elle doit donc être soignée. À cette tenue doit être joint une bonne hygiène.

Attitude

- Le contact client est un aspect primordial lors d'intervention, que ce soit un contact physique ou téléphonique celui-ci doit se faire politesse et entrain.
- Le technicien doit adopter un langage compréhensible pour le client.
- Les intervenants doivent faire preuve de sang-froid quelle que soit la situation et le client.

Interventions / Confidentialité

- Toute intervention devra être détaillée au client avant intervention dans des termes compréhensibles par ce dernier.
- Aucune information confidentielle ne doit être divulguée, copiée en partie ou en totalité.
- Toute installation devra être remise en état après intervention (écran, imprimante, etc...)
- Les problèmes clients devront être résolus au plus vite et un suivi devra être effectué sur le matériel.

6.4 Contrat Infogérance

Objet

La prestation d'infogérance dont ce contrat est l'objet vise à assister le Client dans la gestion de son système informatique.

Maintenance

Prise en charge de la maintenance du parc informatique existant :

- postes individuels (PC) et serveurs,
- services, logiciels (bureautique, anti-virus, etc.),
- supervision (réseaux, matériels, logiciels, etc.)

Conseil

Prise en charge de l'évolution du système informatique :

- infrastructure (machines, câblage, réseaux, etc.),
- logiciels,
- virtualisations (PC, serveurs, LAN, switch, etc.)

Sécurité

Prise en charge de la gestion de la sécurité du système informatique :

- droits d'accès (comptes, fichiers, etc.),
- réseaux (internet, intranet, VPN, etc.),
- sauvegardes

La prestation d'infogérance a pour objectif de réduire au minimum les périodes d'indisponibilité d'un ensemble de matériels et services informatiques, et proposer des améliorations structurelles et/ou logicielles devant permettre un gain d'efficacité du système informatique du Client.

La maintenance

La maintenance du parc informatique du Client couvre notamment :

- la gestion des postes individuels,
- la gestion des serveurs la gestion du réseau interne (intranet),
- la gestion du réseau externe (internet,
- la gestion de la sécurité

La prestation permet ainsi de :

- Limiter la durée des pannes sur les postes individuels :
 - o par indisponibilité logicielle (virus, incompatibilité logicielle, etc.);
 - o par indisponibilité matérielle (diagnostic, dépannage, pièces détachées, etc.),

- maintenir les serveurs opérationnels :
 - o gestion de la sauvegarde et de la restauration des données;
 - o prévention des risques de casse matérielle;
 - o gestion des comptes utilisateurs et des droits d'accès,
 - o aménagement de la configuration matérielle et/ou logicielle en fonction de l'évolution de la société du Client,
- maintenir les réseaux fonctionnels :
 - o suivi et maintenance des dispositifs réseaux (routeurs, firewall, VPN, etc.);
 - o suivi de la connexion aux réseaux.

Le conseil

La prestation d'infogérance comporte une partie d'accompagnement du Client dans l'évolution de son système informatique :

- analyse des besoins et des objectifs,
- proposition de solutions adaptées,
- conseil dans les choix technologiques futurs,
- estimation des coûts,
- mise en place des solutions retenues.

Cette partie de la prestation s'effectue par des demandes spécifiques et préalables du Client.

Les formules d'intervention

Il y a deux types d'interventions :

1. les interventions programmées (au moins 5 jours ouvrés après la demande d'intervention),
2. les interventions urgentes (moins de 5 jours ouvrés après la demande d'intervention).

Pour chaque type d'intervention, il y a deux modes :

1. sur site : l'expert technique du Prestataire intervient directement chez le Client, en se déplaçant sur le site le plus approprié pour l'intervention (dans le cas où le site d'intervention se trouve à une autre adresse que celle du Prestataire les éventuels frais de déplacement, de restauration et d'hébergement seront facturés en sus du présent contrat; en outre toute intervention du Prestataire d'une durée inférieure à une demi-journée sera comptabilisée forfaitairement à une demi-journée);
2. à distance : l'expert technique du Prestataire intervient à distance pour le Client, en se connectant (à l'aide d'un système réseau adapté et sécurisé) à une machine informatique du Client (poste individuel ou serveur) à partir de laquelle il peut intervenir.

Pour chaque type et mode d'intervention, la durée constatée est comptabilisée dans une seule unité de temps, dont la nature et le nombre sont déterminés au moindre coût pour le Client :

- par journées, soit un total de 7 heures d'intervention,
- par demi-journées, soit un total de 3,5 heures d'intervention,
- par heures.

Obligations et responsabilités

Dans le cadre de la prestation d'infogérance dont ce contrat est l'objet, le prestataire sera soumis à la seule obligation de moyens.

Néanmoins à tout moment le Client a la possibilité de demander une obligation de résultat pour une réalisation particulière, appelée Forfait; dans ce cas il en avisera le Prestataire qui lui remettra une étude et un devis séparés.

Excepté le cas d'une faute du Prestataire, le Client renoncera à rechercher la responsabilité du Prestataire en cas de dommages survenus aux fichiers, mémoire d'ordinateur, ou tout autre document, matériel ou programme qu'il pourra confier au Prestataire dans les travaux que celui-ci devra exécuter.

Secret professionnel et propriété intellectuelle

Tous les renseignements, documents, études, paramétrages et codes d'accès auxquels participe le Prestataire ainsi que les travaux objets de la présente prestation, sont strictement confidentiels et de ce fait, couverts par le secret professionnel. Ils seront restitués en intégralité au Client à la résiliation de la prestation sur simple demande, ainsi que toutes les pièces accréditives ou d'autorisation de circulation sur le site d'intervention du Client qui auraient été fournies au Prestataire au début et dans le courant de la prestation.

Le produit de la prestation devient la propriété du Client. Tous les droits de propriété intellectuelle portant sur les travaux réalisés par le Prestataire, notamment les droits d'usage, de production, de modification, d'adaptation sont cédés au Client, pendant la durée de protection légale et en tout pays. En contrepartie, le Prestataire aura le droit d'utiliser le savoir-faire acquis au cours de l'exécution du présent contrat.

Tarifs au 01/01/2017

Prix unitaire HT

- Intervention programmée Journée 315€
- Demi-journée 155€
- Heure 45€
- Intervention urgente Journée 385€
- Demi-journée 192€
- Heure 55€

Durée du contrat - Résiliation

Le présent contrat est conclu jusqu'au 31 décembre de l'année en cours. Il sera tacitement reconduit annuellement à son expiration, en tenant compte toutefois des éventuelles révisions de prix successives depuis sa conclusion.

Toute partie pourra mettre un terme au présent contrat à tout moment sous réserve de notifier sa décision par lettre recommandée avec accusé de réception à l'autre partie, avec un préavis au moins égal à trente (30) jours. La résiliation du présent contrat s'effectuera sans préjudice des dispositions relatives aux cessions de droit de propriété intellectuelle du présent contrat, qui conserveront en conséquence toute leur force et leur portée.

Règlement des différends

Au-delà des plafonds définis par la police d'assurance citée au chapitre 5.2 et en cas de condamnation à quelque titre que ce soit, les sommes éventuellement demandées au Prestataire ne pourraient être supérieures à la valeur annuelle du

montant de la prestation d'infogérance pour le Client plaignant. Dans le cas d'un contrat dont l'ancienneté est inférieure à 12 mois, le plafond des sommes exigibles est fixé à trente mille euros. Le présent contrat est soumis à la loi française. En cas de litige et à défaut d'accord à l'amiable, compétence expresse sera attribuée au Tribunal de Commerce de Bobigny (93), nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence.

6.5 Devis



IT SOLUTION
21 Allée de Chaminaux
33000 Bordeaux
France
Tél : 05 56 54 34 67
Fax : 07 60 57 17 72
34404958000030

DEVIS N° 25553356
Date d'émission : 26/10/2017

Code client : AUTOCONCEPT
3 Rue du Colisée
33000 Bordeaux
France
05 56 67 45 24

DEVIS RENOUVELLEMENT DU PARC INFORMATIQUE

Les prix sont valables jusqu'au 31/12/2017

Référence	Désignation	Quantité	Unité	Prix U HT	Montant HT	TVA %
000244	PC Fixe (Acer Aspire XC-230) + Écran + Office 365	68.00	Pcs	366.00	24 888.00	20.00
000256	PC portable (Lenovo IdeaPad 110-15ACL) + Office 365	6.00	Pcs	308.32	1 849.92	20.00
000214	Onduleur (EATON ELLIPSE ECO 1600)	1.00	Pcs	220.79	220.79	20.00
000355	Serveur (LENOVO system X3650 M5)	1.00	Pcs	1 874.00	1 874.00	20.00
000365	Pare-feu (ASA 5505- UL)	1.00	Pcs	541.00	541.00	20.00
000389	WD RED 4 To SATA 6Gb / s	3.00	Pcs	133.29	399.87	20.00
000345	Logiciel de BackUp (Handy-BackUp)	1.00	Pcs	99.00	99.00	20.00
006450	Windows Server 2012 R2 Standard	1.00	Pcs	345.99	345.99	20.00
000002	Climatiseur	1.00	Pcs	839.00	839.00	20.00
000025	Kit Extincteur	1.00	Pcs	99.99	99.99	20.00
000000	Forfait Prestation	1.00		6 000.00	6 000.00	0.00
Total HT					37 157.56	
Total TVA 20.00%					6 231.51	
Total TTC					43 389.07	
Net à payer (€)					43 389.07	

Règlement
- Date limite : 26/10/2017 (À la réception)
- Mode : Chèque
- Taux d'escompte en cas de paiement anticipé : 30%

Bon pour accord le :
Signature

6.6 Sources

Site web de la CNIL pour la sécurité des mots de passe :

- <https://www.cnil.fr/fr/authentification-par-mot-de-passe-les-mesures-de-securite-elementaires>

Aide pour la charte informatique

- Charte de Sanofi, du CESI, du centre Hospitalier de Bordeaux et de France-Sécurité

Aide pour le contrat d'infogérance

- Contrat de l'entreprise d'infogérance Sibio

6.7 Glossaire

- Active Directory : annuaire de tous les utilisateurs du domaine. Cet annuaire sert aussi à paramétrer des groupes pour gérer des droits.*
- ERP : logiciel de gestion propre à un secteur d'activité. Dans le cas d'AutoConcept, l'ERP est Apigarage par Sage.
- Intranet : réseau informatique privé qui utilise les protocoles d'internet.
- ISO 20000-1 : norme de système de management des services (SMS). Elle spécifie les exigences destinées au fournisseur de services pour planifier, établir, implémenter, exécuter, surveiller, maintenir et améliorer un SMS.
- LAN : « Local Area Network », réseau local. Il s'agit d'un ensemble d'ordinateurs appartenant à une même organisation.

- Pare-feu : logiciel ou matériel permettant de faire respecter la politique de sécurité du réseau. Il surveille et contrôle les applications et les flux de données.
- Proxy : composant logiciel qui joue le rôle d'intermédiaire en se plaçant entre deux hôtes pour faciliter ou surveiller leurs échanges.
- RAID5 : système de stockage de données alliant vitesse de lecture et sécurité. Ce système est couteux en espace de stockage mais est idéal pour les petites structures ne possédant pas beaucoup de données mais ayant déjà fait face à des problèmes de fiabilité de stockage.
- Serveur : dispositif matériel ou logiciel offrant des services (accès internet, stockage de données, boîte mail, contrôle d'accès, ...)
- Switch : dispositif informatique servant à interconnecter plusieurs câbles réseau. Son principe est de diriger les données émises par un pc vers le (uniquement le) pc à qui les données sont destinées.
- VPN : système permettant de créer un lien direct entre des ordinateurs distants. Ce système permet de passer outre d'éventuelles restrictions sur le réseau. Très utiles pour des personnes travaillant à distance souhaitant avoir accès au réseau interne de l'entreprise.