PROJET SaS

Par Sebastien Echeverria
& Nicolas Dupard

PROVIDER

Auto Concept

I. Introduction

1. Présentation d'IT PROVIDER²

est une société spécialisée dans l'infogérance et l'externalisation informatique pour les entreprises. Riche de nos dix années d'expérience et reposant sur une équipe dynamique et qualifiée nous vous proposons des solutions adaptées à vos besoin dans le but de vous concentrer sur votre cœur de métier. Notre société est récemment implantée dans le pôle d'activité Greenopolis de Lyon.

Nous accompagnons scrupuleusement chaque partenaire afin de le conseiller durant son évolution. La pérennité de votre entreprise à la pointe de la technologie est notre priorité.

Nous garantissons des interventions rapides et efficaces faisant ainsi de votre outil informatique une base solide et dynamique.

Nous allons vous présenter dans un premier temps nos missions, la qualité de nos prestations, nos certifications, notre équipe et nos partenaires.

a. Missions

- Analyser l'acquis et vos besoins
- Proposer et installer les meilleures solutions
- Déployer et vous accompagner en permanence
- Effectuer une surveillance continue
- Evaluer et proposer l'évolution technologique

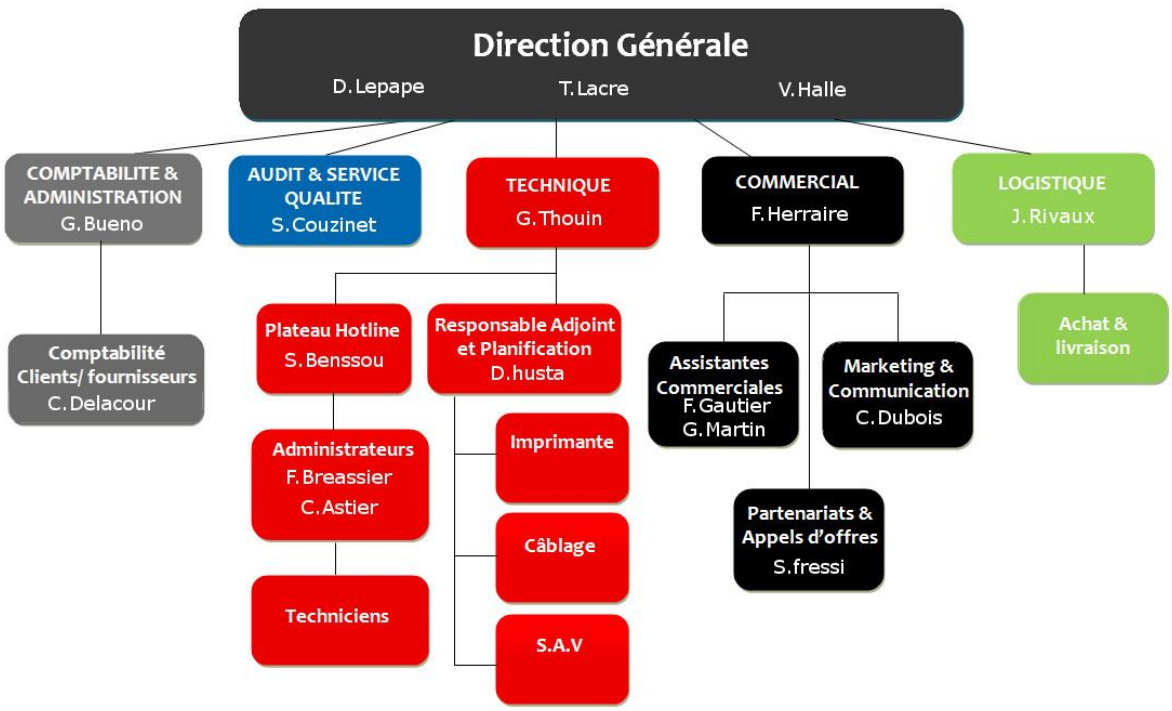
b. Qualité de nos prestations

- Une équipe d'expert maitrisant l'architecture système
- Une veille technologique soutenue
- Une ingénierie appréciée de tous nos partenaires
- Une charte qualité certifiant un service, une écoute et une disponibilité sans faille.

c. Certifications

- **ISO 9001 :** une norme internationale de management de la Qualité au sein d'une entreprise.
- **ISO /IEC 20000 :** une norme de certification des services informatiques, des organisations prouvant le respect des normes de qualité éditées au travers de phases, de contrôles et de procédures de mises en place.
- **ISO 27001 :** une norme qui décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI). Le SMSI recense les mesures de sécurité, dans un périmètre défini, afin de garantir la protection des actifs informationnels.
- **ISO 14001 :** une norme internationale établie par l'organisation internationale de normalisation, qui constitue la référence des organismes pour mettre en place un système de management environnemental. Elle a pour objectif d'aider les entreprises à gérer l'impact de leurs activités sur l'environnement et à démontrer l'efficacité de leur gestion.

d. Notre équipe :



Contact :
@ : it.pro2@gmx.com
Tel : 04.37.730.730
Adresse : ITProvider2, Greenopolis, 24 rue Berjon 69009 Lyon

e. Nos Partenaires :

2. Charte qualité d'IT PROVIDER²

Nous nous engageons à respecter chaque point de notre charte qualité service client.

- ITP² favorise l'infogérance informatique comme la meilleure solution possible de gestion, de suivi et de support de parc informatique pour une entreprise. Le rôle du chef d'entreprise ne devant se limiter qu'à la surveillance et au suivi de la performance de son partenaire d'infogérance spécialiste de l'informatique en charge de son infrastructure.

- Notre Objectif est votre satisfaction. Elle passe par l'accompagnement quotidien, les conseils murement réfléchis d'une équipe d'experts et finalement par une veille technologique.

- ITP² assume la responsabilité de la gestion quotidienne de fonctionnement du réseau informatique, des applications et est disponible pour fournir un support et une assistance rapide aux utilisateurs lorsqu'ils ont besoin d'aide.

- Nous adaptons le service de support et d'assistance informatique pour répondre à vos besoins spécifiques, nous comprenons que vous avez des besoins uniques.

- Un simple appel à notre service d'assistance pour toute demande support informatique pour vous ou vos collègues. Il n'y a pas de boîte vocale ou d'options de téléphone à composer pendant les heures ouvrées, vous serez directement en contact avec une personne qui vous mettra en relation avec la personne la plus adaptée pour répondre à votre requête directement ou vous rappelez rapidement pour arriver à une résolution rapide.

- Nous sommes structurés avec une équipe de support et assistance informatique à taille humaine, vous recevez donc un service personnalisé. Que l'assistance soit fournie par l'assistance téléphonique, en dépannage à distance ou en personne par une intervention sur site, nous bâtissons une relation sur le long terme avec votre entreprise, vous et vos collaborateurs.
- ITP² supervise votre infrastructure en permanence via sa plateforme de supervision et est averti instantanément du moindre problème survenant sur vos serveurs et réseau. Les vérifications quotidiennes de votre système de messagerie, serveurs de réseau, connexion de secours et

d'accès à Internet sont validés avant l'ouverture de votre entreprise. Cela nous permet de corriger les problèmes avant que vos utilisateurs et vous-même débutiez votre journée de travail.

- La vérification régulière de la santé de vos serveurs est un autre exemple de notre service d'infogérance et de gestion proactive de votre infrastructure informatique. Nous veillons à ce que vos serveurs disposent des derniers correctifs de sécurité et sont en bon état de santé.

- Nous garantissons votre sécurité grâce au plan de Sécurisation de données et de notre système de prévention d'intrusion.

- Nous assurons la continuité de service via nos mesures de sauvegarde qui nous permettent d'effectuer la restauration de vos données dans un délai de quatre heures. Le délai d'intervention d'un spécialiste sur site n'excédera pas une heure entre 7h30 et 18h30.

- Durant tout le temps de notre collaboration et même ensuite, toute l'équipe s'engage pour garantir la confidentialité de vos informations, qu'elles soient confidentielles ou non.

- Notre service d'infogérance informatique vous propose un système de forfait afin que vous puissiez bénéficier d'une offre sur mesure selon les contraintes et besoins de votre entreprise.

Quels frais supplémentaires peuvent être facturés?

- L'installation de nouveaux ordinateurs, serveurs et imprimantes est un supplément. Les activités de projet, telles que la création d'un nouveau bureau, implanter un réseau domestique, l'amélioration des applications logicielles et matérielles, créer ou mettre à jour votre site web, les formations, sont cotés sur une base fixée une fois que nous comprenons vos exigences et la portée de votre projet.

Véronique Halle le 9/01/2015

II. Projet SAS

1. Présentation d'AutoConcept et particularité du contrat

AutoConcept est une entreprise exerçant dans le domaine de l'automobile. Elle offre la possibilité d'acheter des véhicules neuf mais aussi d'occasion, et dispose aussi d'un atelier.
Actuellement forte de 83 employés, AutoConcept possède un parc informatique de 70 à 80 postes gérer par deux informaticiens en internes. A noter que l'un des deux informaticiens d'AutoConcept sera recruté suite à l'obtention du marché.

2. Problématique

AutoConcept souhaite externaliser les prestations informatiques aujourd'hui exécutés par deux informaticiens en internes suite à de nombreux problèmes rapporté dans le compte-rendu du service commercial.
On y trouve :

- Lenteur de certains postes.
- Crash disque du poste d'un commercial : perte d'exploitation de 80 000€.
- Intrusion d'un client sur un pote d'une commerciale dépourvu de mot de passe.

Ainsi que des plaintes des utilisateurs sur le service informatique :

- Délais d'intervention : un poste d'une secrétaire commerciale est parti en SAV durant 2 jours. Elle n'a pas pu terminer un document pour conclure en affaire. Perte : 60 000€.
- Messages intempestifs de "version de Windows pirates".
- Une intervention urgente planifiée pour le lundi 10h a été traitée le mercredi à 10h.
- Etc...

3. Préconisations

Après avoir pris connaissance des problèmes qui touchent le parc informatique d'AutoConcept, la société IT Provider² a rédigé un rapport d'étude technique pour répondre aux besoins du concessionnaire. Cette étude se divise en plusieurs grandes parties. La première étant une synthèse sur l'utilisation de l'outil informatique en entreprise, elle traite les points sensibles que sont : Les mots de passes, la messagerie électronique, l'utilisation d'internet et des programmes en entreprise ainsi que la confidentialité des données. Ensuite sera présenté la charte informatique que chaque salarié devra lire attentivement, parapher et signer. Puis vous pourrez prendre connaissances du plan de sécurisation et de sauvegarde des données, aussi bien sur le côté technique, organisationnel qu'humain. Pour finir, il vous sera expliqué le principe de la Hot Solution avec ses nombreux avantages.

III. Etude technique

1. Note de synthèse sur l'utilisation de l'outil informatique en entreprise

Cette note définit les règles de bon usage des ressources informatiques de « auto concept », en assurant un équilibre entre les besoins d'interconnexion du système d'information, les exigences d'intégrité, de disponibilité, de confidentialité associées et le respect des contrats, lois et règlement en vigueur.

Elle s'applique à toutes personnes travaillant pour la société à titre permanent, temporaire ou intérimaire, qui utilise ou gère les ressources informatiques mise à disposition par auto concept

Ces ressources informatiques comprennent les serveurs, stations de travail, micro-ordinateurs, modems, données et logiciels, service commun et tous les réseaux de communications (interne ou externe), qui permettent d'accéder aux informations propres à « auto concept », ainsi qu'aux informations situées hors sites de l'entreprise. L'ensemble de ces ressources est nommé Système d'Information (SI).

a) Mot de passe

L'utilisateur est dans l'obligation de choisir un mot de passe en conformité avec la procédure d'autorisation et de délivrance dans l'entreprise.

Une fois intégré dans l'entreprise, un identifiant et un mot de passe seront communiqués via téléphone par un technicien de la société qui s'occupe de l'infogérance. L'utilisateur devra ensuite changer le mot de passe temporaire à sa première connexion.

L'utilisateur est seul responsable de son mot de passe. Il est strictement confidentiel et ne dois pas être noté ou ne pas être accessible aux autres utilisateurs.

L'entreprise se réserve le droit d'accéder à la messagerie et aux dossiers d'un utilisateur en cas d'absences prolongées afin d'éviter toutes discontinuité dans le traitement et le fonctionnement de l'activité de la société.

L'utilisateur ne doit en aucun cas enregistrer son mot de passe dans un processus d'authentification automatique.

Pour des raisons de sécurité, l'utilisateur devra changer régulièrement, tous les 3 mois, son mot de passe. L'utilisation d'ancien mot de passe est interdite. Dans le cas où

la confidentialité du mot de passe est compromise, l'utilisateur est dans l'obligation de le changer.

b) Messagerie électronique

Les services de messagerie de « auto concept » ne doivent, en aucun cas, être utilisés pour envoyer des courriels à caractère diffamatoires ou à des fins de harcèlement, d'achat non autorisé, ou pour émettre des opinion qu'elles soient diffamatoires ou pas au sujet des salariés, prestataires, fournisseurs, partenaires ou client de la société.

L'utilisateur devra classer tous les courriers électroniques à caractère personnel de sa messagerie professionnelle.

L'utilisateur doit être vigilant et ne doit pas ouvrir les pièces jointes provenant de tiers inconnu ou tout simplement inattendues. Ces pièces jointes représentent une menace pour l'ensemble du site. Elles contiennent des virus, des vers ou des chevaux de Troie. Leur signalement doit être immédiat aux services informatiques ou au responsable hiérarchique. Il est formellement interdit de déplacer, d'exécuter, copier ou transférer ces menaces à l'intérieure ainsi qu'à l'extérieure de la société.

L'utilisateur doit adopter un comportement raisonnable en nettoyant régulièrement sa messagerie des courriels non indispensables. Cette demande a pour but d'éviter que les boites de messagerie occupent de plus en plus de place sur le serveur inutilement.

c) L'utilisation d'internet

Le contenu de l'information sur l'internet ne peut être contrôlé.
La société ne pourra être responsable de tout contenu consulté ou téléchargé. L'utilisation d'internet doit être conforme aux règles régis par la société et intervenir dans le cadre de l'exécution normale des responsabilités professionnelles de l'utilisateur.

Le non-respect des règles et mesures de sécurité engage la responsabilité personnelle de l'utilisateur et l'expose éventuellement, de manière approprié et proportionné au manquement commis aux sanctions disciplinaires définies par le règlement intérieure et, le cas échéants, au licenciement du salarié concerné. Toute activité illégale pourra être signalée aux autorités compétentes.

d) Logiciels et programmes

L'utilisateur est responsable de son poste de travail et doit s'assurer qu'aucune tentative n'est menée pour désactiver ou contourner les logiciels installés par la société comme les anti-programmes malveillants, les pares feu, le proxy et les services de mise à jour automatique.

L'utilisateur est conscient qu'il lui est interdit de télécharger depuis internet sur un des équipements informatique de la société des logiciels pour lequel l'entreprise n'a pas de licence. Cette interdiction comprend les logiciels gratuits, les logiciels partagés, les

économiseur d'écran, les barres d'outils et ou tous les autres programmes à leur disposition.

Seuls les administrateurs sont habilités à valider et à installer des logiciels sur les équipements informatiques de l'entreprise.

Le piratage de logiciel est strictement interdit (voir loi charte informatique texte de référence). Le piratage de logiciel augmente le risque de virus et de perte de données, aucun support technique ne propose d'assistance pour des logiciels non-couverts par une licence valable. Une poursuite pour piratage affecte l'image et la réputation de l'entreprise.

e) L'utilisation d'internet en entreprise

Interdire l'utilisation d'internet aux employés pour des fins professionnelles sur le lieu de travail est une mission impossible tant l'utilisation des outils informatique est indispensable aujourd'hui.

Les employeurs ont le droit de limiter l'utilisation d'internet ou de filtrer la connexion à condition de prendre quelques précautions de mise en place. (Voir charte informatique : pare-feu)

La CNIL, gendarme des libertés informatiques, nous informe à travers une guide pour les employeurs et salariés qu'il est impossible d'interdire de « manière générale et absolue » l'utilisation d'internet à des fins personnelles

Les origines du filtrage proviennent de plusieurs textes de loi :
.L'arrêté 27 juin qui définit le filtrage comme la mise en correspondance de formes selon l'ensemble prédéfini de règles ou de critères.
Le droit communautaire reconnait depuis plus longtemps encore le droit de filtrer et ce depuis 1999 à travers plusieurs décisions.
La circulaire relative à l'usage d'internet dans le cadre pédagogique et de protection des mineurs du 18 février 2004 prévoyant « la mise en œuvre d'outils de filtrage dans les établissements ou les écoles.
Loi HADOPI du 12 juin 2009 favorisant la diffusion et la protection de la création sur internet.

La nécessité de filtrage s'est imposée naturellement comme l'une des solutions à l'accès des contenus illicites dans tous les domaines.

La mise en place d'une politique de surveillance des connexions des salariés suppose la collecte, le stockage et le traitement d'information d'identification de personne physique. Dès lors, la création d'un tel fichier doit être conforme au règlement de la CNIL. Sauf si l'entreprise dispose en interne d'un « correspondant CNIL » charger de veiller au respect de la loi, l'employeur devra déclarer auprès de la CNIL la création de ce fichier. Il s'engagera aussi à utiliser et administrer ces données conformément à la loi (respect des objectifs, durée de vie, information des personnes fichées, confidentialité des données).

Selon l'article L121-8 du Code du travail la mise sous surveillance d'un salarié ne peut se faire à son insu.
Le code du travail prévoit une information individuelle (art L1222-4) et collective (art L432-2) des salariés sur l'existence d'un traitement contenant des données personnelles les concernant. Il faut l'avertir grâce à la charte informatique jointe au règlement intérieure de son contrat de travail et la mettre en évidence dans les locaux de l'entreprise.
Art L1222-4 Code du travail : Aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance.
Art L432-2 : Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail du personnel

f) Confidentialité des données

- Respect de la vie privée du salarié

Il est acquis que tout salarié a droit au respect de sa vie privé sur son lieu de travail et pendant son temps de travail (art 9 du code civil et art 8 convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales).

La surveillance des fichiers informatiques : les fichiers détenus dans l'ordinateurs d'un salarié sont par principe professionnels sauf s'ils sont identifiés comme personnels par le salarié. Un salarié qui empêche son employeur d'accéder à son ordinateur, notamment en installant un code ou un procédé de cryptage, encourt un licenciement pour faute grave, quel que soit le contenu des fichiers sur son ordinateurs, l'employeur ne peut procéder à leur ouverture sauf en sa présence et après l'avoir prévenu ou si il existe un risque particulier pour l'entreprise (acte de terrorisme, danger économique, espionnage industriel, concurrence déloyale)

- L'accès aux mails :

Les mails sont largement couverts par le secret des correspondances dès lors qu'ils sont classés dans un fichier intitulé « personnel » et ne peuvent par conséquent constituer un moyen de preuve justifiant le bien fondé d'un licenciement.
C'est au salarié d'identifier les messages qui sont personnels, un message envoyé ou reçu depuis un ordinateur professionnel revêtant par principe un caractère professionnel sauf s'il est identifié comme étant personnel dans l'objet du message par exemple. (Cas, soc 30 mai 2007, n° 05-43102).
L'employeur doit donc tolérer que ses salariés utilisent à des fins personnelles le matériel informatique qu'il met à leur disposition pour un usage professionnel. Un principe affirmé pour la premières fois en 2001 dans le célèbre arrêt Nikon.

- Contrôle de la connexion internet :

Toutes les connexions internet du salarié sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher afin de les identifier même en dehors de la présence du salarié (Cas. Soc, 9 juill. 2008, no 06-45.800) et le restent malgré, par exemple, l'inscription de site sur la liste des « favoris » (Cas, soc, 9 févr. 2010, no 08-45.523). Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés pour en obtenir régulièrement communication et des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex : la police, le fisc). La communication d'information à des personnes non-autorisées est punie de 5 ans d'emprisonnement et de 300000 euros d'amende.
La divulgation d'information commise par imprudence ou négligence est punie de 3 ans d'emprisonnements et de 100000 euros d'amende Art. 226-22 du Code pénal.

- Respect de la clause de confidentialité

La clause de confidentialité a pour finalité de déterminer le cadre juridique des informations confidentielles, quel que soit leur nature, dans un contrat. Elle sert à protéger les parties au contrat, afin d'éviter la divulgation d'informations particulières qui si elles étaient révélés, causeraient un préjudice à l'une des parties, voire remettrait en cause le contrat, lui-même, ainsi que la collaboration entre les parties. En effet, lorsque des personnes entrent en relation d'affaire, elles se doivent de partager certaines informations capitales pour la survie de leur activité (secret de fabrication, savoir-faire) ou personnelles (données bancaire, données nominative) ou commerciales (chiffres, études statistiques, stratégie marketing, fichier clientèles, méthodes). Elles doivent également prévoir les mesures pour éviter de mettre en péril leur activité. C'est ainsi que la clause de confidentialité organise la protection de toutes ces informations, leur communication, leur droit de reproduction éventuelle, ainsi que les droits de propriété intellectuelle qui y sont attachés, jusqu'au terme des relations contractuelles, voir au-delà.

Dans le système juridique français, il n'existe pas à proprement parler de protection légale de « la donnée confidentielle ». L'entreprise ne les protège contre le risque de divulgation que si elles le juge opportun. La protection de ces données est donc essentiellement contractuelle.

Il en est de même du code du travail. Les conséquences en cas de non-respect de cette obligation sont en pratique, fixé par la jurisprudence. L'employeur lésé en raison du non-respect de l'obligation de confidentialité peut, pendant la durée du contrat de travail, réclamer à l'employé des dommages et intérêts. C'est seulement lorsque le salarié révèle des secrets professionnels que la loi sanctionne : l'article L1227-1 du code du travail ; repris dans l'article L621-1 du code de la propriété intellectuelle, prévoit une peine d'un an d'emprisonnement et de 30000 euros d'amende et le cas échéant la perte des droits civiques et de famille, prévue à l'article 131-26 du code pénale, pour 5 ans maximum.

Des sanctions spécifiques, propre à l'entreprise, peuvent néanmoins être prévues par un règlement interne (exemple : des amendes, des avertissements). Un manquement grave à l'obligation de confidentialité peut même mener au licenciement pour motif urgent. Enfin, si l'employé agit dans l'intention de nuire à l'employeur ou d'en tirer illégalement profit pour lui-même ou pour autrui, il s'expose à une peine de trois mois à trois ans d'emprisonnement et à une amende.

2. Charte informatique

Préambule

Les systèmes d'information sont aujourd'hui au cœur de l'entreprise, et ce, quels que soient son secteur et ses domaines d'activités. De plus en plus d'employés travaillent ainsi au quotidien dans l'entreprise avec un accès direct vers l'extérieur : généralisation de l'accès à Internet sur les postes informatiques et des messageries professionnelles.

Si l'utilisation de l'outil informatique et internet dans l'entreprise est indispensable, elle peut néanmoins très vite devenir source d'abus, de litige, mettre en danger l'utilisateur et engager directement la responsabilité de l'employeur.

Afin de pallier à tous ces problèmes il existe des lois pour protéger le salarié et l'employeur mais aussi et surtout il est nécessaire de fixer des règles claires pour responsabiliser les différents acteurs.

1) Sécuriser l'accès au compte

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification, (c'est-à-dire un nom d'utilisateur et un mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas le communiquer.

Chaque mot de passe doit être modifié à intervalle régulier. Il doit, pour être efficace, comporter plus de 8 caractères, des chiffres et des lettres, majuscules et minuscules, caractères spéciaux (?*% etc…) et ne doit pas correspondre à un mot existant dans le dictionnaire.

2) a) Courrier électronique

Les éléments de fonctionnement de la messagerie à considérer sont les suivants.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf si elle est crypter.

Il est tolérer d'utiliser des services d'un site web spécialisé dans la messagerie, mais il est préférable de se servir d'un logiciel, comme Outlook.

Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de deux mois et il existe des copies de sauvegarde pendant une période de un an.

b) Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

A ce titre, les salariés devront identifier leurs messages et fichiers personnels de façon à ne pas les confondre avec les messages reçus à titre professionnel : qualification par l'objet, création d'un répertoire spécifique dédié au contenu privé.

c) Contrôle de l'usage

Dans l'hypothèse la plus courante, le contrôle éventuellement mis en œuvre porte sur :

-Le nombre de messages échangés
-La taille des messages échangés
-Le format des pièces jointes

3) Utilisation d'Internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

-De communiquer à des tiers des informations techniques concernant son matériel
-De diffuser des informations sur l'entreprise via des sites Internet
-De participer à des conversations en ligne (dit "chat")

4) Utilisation d'Internet à des fins privées

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel (saturation de la bande passante)

5) Pare-feu

Le pare-feu vérifie tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de la messagerie électronique et de la navigation sur Internet.

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

-De la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature
-Des messages envoyés et reçus expéditeur, destinataire(s), objet, nature de la pièce jointe.

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale ou contenant des données jugées comme offensantes.

6) Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à doubler le système en cas de défaillance.

Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il e reste une copie sur le serveur.

7) Sanctions

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entrainer à son encontre des avertissements, des limitations ou suspensions d'utiliser, tout ou partie, du système d'information et de communication, voir des sanctions disciplinaires, proportionnel à la gravité des faits.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier.

8) Textes de référence

Les années récentes ont vu l'émergence d'un droit spécifique aux systèmes de traitement de l'information. Voici trois aspects ainsi que les textes correspondant.

-Loi sur la fraude informatique :

Elle concerne les atteintes aux systèmes de traitement automatisé des données et a défini des incriminations spécifiques à ces systèmes. Les peines vont de deux à cinq ans d'emprisonnement et de 30 000 à 75 000€ d'amande.

-Loi relative au droit d'auteur

Les programmes d'ordinateur sont assimilés à des œuvres littéraires. Ils sont donc protégés pendant la vie de l'auteur, plus 70ans. Au pénal, la contrefaçon est punie de cinq ans d'emprisonnement et de 500 000€ d'amendes.

-Loi "Informatique et Libertés

Elle date de janvier 1978 et concerne les informations nominatives, c'est-à-dire celles qui permettent l'identification des personnes auxquelles elles s'appliquent. Dans le nouveau Code Pénal, les articles 226-16 à 226-22 rappellent les incriminations possibles et les peines qui leur sont associées, c'est-à-dire cinq ans d'emprisonnement et 300 000€ d'amende.

9) Information des salariés

La présente charte est communiquée à chaque salarié. IT Provider² est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC (nouvelles technologies de l'information et de la communication). Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

Fait à _____ _____ le __/__/__.

Nom :
Fonction :
Signature :
Précédée de la mention « lu et approuvé »)

3. Le plan de sécurisation des données et de sauvegarde des données

Afin de se prémunir contre les risques concernant la sécurité des fichiers, la loi "informatique et libertés" du 6 janvier 1978 prévoit que « Auto Concept», doit garantir la sécurité des données qu'elle utilise. Pour cela, les détenteurs de ces fichiers doivent mettre en application un ensemble de mesures techniques, organisationnelles et humaines.

- Technique : nous contrôlerons la sécurisation des infrastructures par le cryptage des données et par la mise en place de solutions techniques afin de pouvoir renforcer le niveau de sécurité de votre système d'information.

- Organisationnelle : Nous managerons une politique de sécurisation globale et centralisée ainsi qu'une définition des responsabilités et rôles des différent acteurs. Nous élaborerons un processus de gestion des incidents et des sinistres.

- Humain : la sécurisation des fichiers passe essentiellement par la sensibilisation des utilisateurs et responsables afin d'instaurer une culture de sécurité dans l'entreprise via une charte informatique

Après un audit du parc informatique de « auto concept », nous avons pu définir les points capitaux du contrat d'infogérance qui nous lie :

- Une gestion totale du réseau informatique (installation et paramétrage).
- Un suivit d'audit régulier et des conseils permanents.
- Un accès à la télémaintenance illimité, du lundi au samedi de 9h00 à 18h00 sans interruptions.
- Des interventions sur site en cas d'urgence.
- Un entretien régulier du parc informatique.
- La livraison et installation de logiciels et matériels si nécessaire. (L'informaticien « d'auto concept » se chargera des opérations de bas niveau sur site, il aura un accès VPN à notre structure pour la création de Ticket)

Pour sécuriser le système informatique et la sauvegarde de données, nous vous proposons une solution à mettre en place en plusieurs étapes.

a. Centralisation des données

La centralisation des données présente divers avantages pour le client. Elle permet l'existence d'une base de données unique, accessible aux utilisateurs authentifiés. L'intégrité des données est ainsi garantie grâce à un exemplaire unique pour tous. Et leur accessibilité devient plus facile et plus sécurisée.

Pour ce faire, nous allons mettre en place un lecteur réseau virtuel. Il permettra de centraliser les données. De plus, nous allons créer des dossiers communs propres à chaque groupe d'utilisateur. Ainsi que un dossier personnel à chacun des utilisateurs. Cela permettra à tous les utilisateurs de stocker leurs données professionnelles sur le lecteur réseau virtuel, dans de façon organisée.

b. Active Directory (AD)

La mise en place d'identifiant et d'un mot de passe et obligatoire. Cela permet de protéger les utilisateurs d'éventuelle intrusion sur leurs ordinateurs. Et donc de protéger leurs données personnelles et professionnelles stockées sur leurs postes.

Une liste des employés sera demandée à « auto concept » afin de créer une base d'utilisateurs. L'identifiant d'un utilisateur sera composé des 7 premières lettres de son nom de famille et des 3 premières lettre de prénom afin que le nombre de caractère soit de 10 (pour tout cas particulier, voir notre hotline). Les mots de passe, lors de la mise en place de l'AD, seront communiqués par téléphone via notre hotline seulement à l'utilisateur concerné. Il sera par la suite dans l'obligation de changer de mot de passe.

Afin qu'un mot de passe soit efficace, il doit être créé à partir d'une règle de création de mot de passe :

- Un mot de passe doit avoir une longueur minimale de 8 caractères.
- Au moins une lettre minuscule
- Au moins une lettre majuscule
- Au moins un nombre
- Au moins un caractère spécial (?, *,%, Etc.)
- Les mots de passe doivent être changés, au minimum, tous les 120 jours :

Nous mettrons en place une règle permettant d'obliger les utilisateurs à changer leur mot de Passe tous les trimestres.

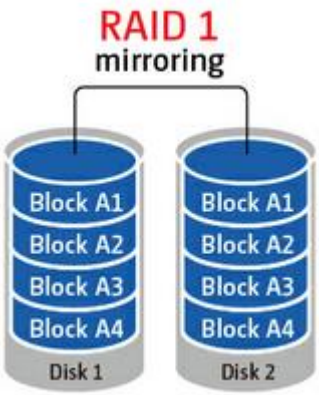
Chaque utilisateur fera partie d'un groupe en fonction du poste qu'il occupe dans l'entreprise. Dans le but de donner des droits d'accès à certains répertoires du lecteur réseau mis à disposition des utilisateurs.

Pour des raisons de protection des données et du système informatique, seul les administrateurs sont autorisés à installer ou modifier les logiciels.

c. Système de sauvegarde

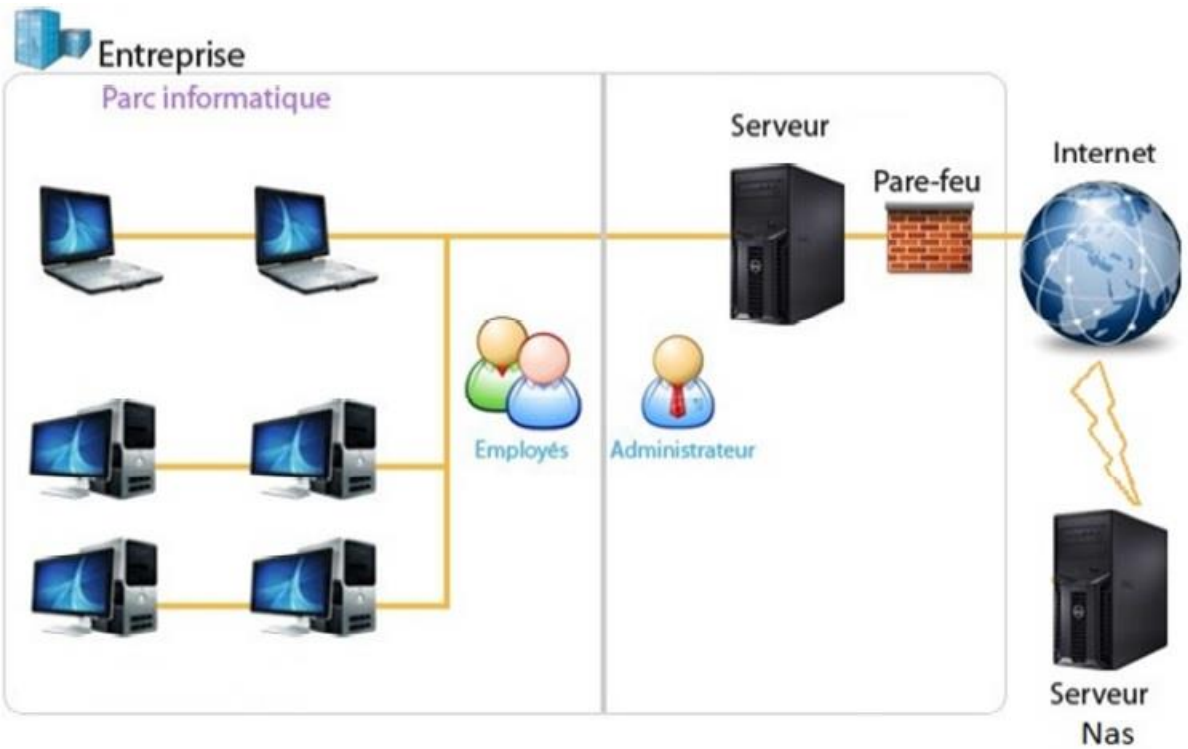
Il existe plusieurs matériels pour effectuer les sauvegardes des données logiques. Il est primordial d'investir dans un moyen de sauvegarde efficace puisque une perte de données peut couter très chère à votre entreprise comme vous avez pu le constater. De nombreuses méthodes existent avec pour chacune d'elle des avantages et des inconvenants. Le matériel que nous avons choisi pour votre entreprise est le disque dur.

En terme de mesure de sauvegarde immédiate, nous mettrons en place un système de RAID 1, il est assez parlant puisqu'il se nomme également « en miroir ».Pour ce niveau, il faut deux disques durs de même capacité (ou un nombre pair de disques).Ce qui est écrit sur un disque, est copié à l'exacte sur le second, les deux disques sont identiques d'où le terme de miroir. Si un disque vient à tomber en panne, aucun souci, le second est sa copie conforme et les données sont toujours là. Avec ce niveau, tout est axé sur la sécurité au détriment de la vitesse d'écriture, en effet, il faut enregistrer deux fois le fichier au lieu d'une en cas normal. Voici le principe de fonctionnement :



Ce que nous vous proposons, c'est d'effectuer ces sauvegardes à une heure fixe tous les jours, en fin de journée. Ces sauvegardes s'effectueront dans vos locaux grâce à vos serveurs, nous mettrons alors en place ce système de raid.

Dans le but de minimiser les risques, nous proposons l'installation d'un espace de stockage en réseau qui sera physiquement situé dans nos locaux, dans la salle serveur, pour un coût de 133 € seulement. Ce serveur NAS, aura pour rôle de retrouver vos sauvegardes si un dégât matériel devait arriver dans vos locaux.



d. Logiciels et matériels de protections

- L'Antivirus, Antimalware, Antispyware

Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (virus, fichiers espions, logiciel malveillant).
Ces derniers se basent soit sur l'exploitation de failles de sécurité, soit il s'agit de programmes qui modifient ou suppriment des fichiers. Leurs cibles sont des documents de l'utilisateur mais aussi des fichiers nécessaires au bon fonctionnement de l'ordinateur.

C'est pour ces raisons que la présence d'un antivirus est **obligatoire**. Il est systématiquement installé par l'administrateur qui installe le poste. Les mises à jour sont faites automatiquement

Nous vous proposons d'installer Mcafee virusScan entreprise 8.8 pour le prix de 4.5 euros par poste et pour une durée de 3 mois. Il propose une défense optimale contre les logiciels malveillants, une protection proactive contre les attaques, une gestion centralisée simplifiée et des fonctions de sécurisation améliorées optimisées par McAfee Global Threat Intelligence.

- FireWall

Un pare-feu (appelé aussi coupe-feu, garde-barrière ou firewall en anglais), est un système permettant de protéger un ordinateur ou un réseau d'ordinateurs des intrusions provenant d'un réseau tiers (notamment internet). Le pare-feu est un système permettant de filtrer les paquets de données échangés avec le réseau, il s'agit ainsi d'une passerelle filtrante.

Nous vous proposons d'installer un firewall « Cisco ASA 5512-X Firewall Edition » pour le prix de 2 388,00 € TTC. Il possède toutes les dernières technologies en matière de sécurité ainsi qu'un accès VPN.configurable.

- Proxy

Un Proxy est un terme informatique général qui désigne un composant logiciel qui se place entre deux autres pour faciliter ou surveiller leurs échanges, il est presque systématique en entreprise ou dans les établissements scolaires que l'accès internet se fasse à travers un proxy. L'internaute ne voit pas la différence, sauf quand il tente de naviguer sur un site interdit, auquel cas il pourra recevoir un message d'erreur.

Le proxy sera installé par nos soins sur le firewall. Une boite de dialogue s'ouvre et demande un identifiant et un mot de passe d'ouverture de session de Windows quand l'utilisateur souhaite pour la première fois de la journée surfer sur internet.

- Anti spam

Un anti spam sera installé sur votre serveur de messagerie. On utilisera « vade retro dekstop », il est gratuit et sans engagement.

e. VPN

Dans les réseaux informatiques et les télécommunications, le réseau privé virtuel est vu comme une extension des réseaux locaux. Il préserve la sécurité logique que l'on peut avoir à l'intérieur d'un réseau local.

Le VPN est une interconnexion de réseaux locaux via une technique de « tunnel ». Ce réseau est dit virtuel car il relie deux réseaux « physiques » (ou locaux) par une liaison non fiable (Internet). Cette connexion reste privée car seuls les ordinateurs des réseaux locaux peuvent accéder aux données en clair.

Le but étant, de fermer le réseau local pour que seuls les ordinateurs de l'entreprise y aient accès, ce qui protègera les données de l'entreprise.

Ce VPN sera mis en place quand nous aurons la liste complète des commerciaux, des personnes souhaitant avoir cet accès et que le futur devis sera validé. L'accès distant des utilisateurs disposant d'une clé 3G (25euros sans forfait) fournis sera configuré par nos soins. Les Commerciaux disposants d'un ordinateur portable seront contactés par nos équipes pour l'installation et la validation de l'accès VPN.

f. Sécurités Physique

Pour assurer une bonne efficacité du système informatique, il ne suffit pas de sécuriser les données fichiers, il faut également protéger tout le système, des intrusions extérieures. Pour cela, il faut fermer l'accès à la salle par une serrure ou une porte à code. Seules les personnes désignées par la direction pourront y pénétrer (responsable informatique). Le service de nettoyage n'a aucun droit d'accès à cette salle. Le nettoyage est assuré par le futur ou présent système de ventilation.

Votre local technique doit contenir uniquement du matériel informatique actif ou passif (switch, routeurs, serveurs) et nécessite donc une température régulée, soit par une simple ventilation, soit par une climatisation si les conditions climatique s'avèrent délicates.

Nous conseillons une limite de température de 20°dans la salle. L'installation d'une sonde dans la baie afin que le système de ventilation agisse en conséquence sera prévu quand le locale sera conforme.

Afin de protéger le local du serveur contre les risques d'incendie il faut obligatoirement un extincteur dans le local. Il existe différents types d'extincteurs pour chaque type de feux:

- A : feux de combustibles solides: bois, papier, linge, plastique, caoutchouc…
- B : feux de combustibles liquides et gaz inflammables: graisse, huile, peinture, solvants…
- C : feux d'équipements électriques sous tension: boîte à fusibles, moteur électrique, fils, panneaux électriques…
- D : feux de métaux: magnésium, aluminium…

Pour une salle Serveur il est préférable d'utiliser les extincteurs (CO^2) pour les feux de types A et C.

Des onduleurs certifiés doivent être mise en place et vérifié par un professionnel au maximum tous les 5 ans.

Pour la mise en conformité de votre salle serveur, nous vous proposons les services de notre prestataire spécialiste (privé). Il rédigera un devis après un audit de votre salle serveur.

g. Qualité service client

La continuité de service est assuré en cas de panne grâce au service de Hotline avec une prise en main à distance, tenu par des techniciens et des ingénieurs, disponible du lundi au samedi de 7h30 à 18h30. Le dépannage sur site de J+0 à J+2, en fonction du type de pannes.

La relation client est gérer par une gestion de parc qui permet de rendre accessible toutes les demandes que vous avez pu nous faire. Les logiciels complets que nous utilisons sont GLPI et DiaClient :

« GLPI » est une solution open-source afin de gérer le parc informatique. Celui-ci est une application Full Web qui permet de gérer l'ensemble de l'inventaire des composantes matérielles ou logicielles d'un parc informatique.

La gestion d'incidents est gérée par l'outil « DiaClient ». La hotline génère automatiquement un ticket d'intervention, lors d'un appel ou d'une remonté d'incident. Le ticket est ensuite traité par les autorités compétentes. L'utilisateur recevra un courriel de confirmation dans sa boite mail afin de lui indiquer que sa demande est bien prise en compte. Il en recevra un autre à la clôture du problème.

Ce logiciel va permettre de résoudre une importante partie des plaintes des utilisateurs qui sont citée dans le compte rendu service commercial.

h. Mise à jour du parc informatique de « auto concept »

Lors de notre audit, nous avons constaté que certains postes de travail ne possédaient pas le même système d'exploitation, étaient défaillant ou nécessités un remplacement

Une mise à jour du parc informatique s'impose pour les raisons suivante :

- Système d'exploitation XP n'est plus sûr, Microsoft ne fournit plus de mise à jour depuis le 8 Avril 2014. Un changement pour le système d'exploitation Windows 7 est notre solution.
- Le renouvèlement des postes ne supportant pas « Windows 7 » de par leur capacité technique insuffisante (mémoire vive < 4Go, processeur vielle génération et capacité disque dur < 20Go)
- Un poste de travail défaillant

Un inventaire de votre parc informatique sera créé sur la base de GLPI. Cet inventaire nous permettra de vous aviser des postes à changer ainsi que d'un devis les concernant. Nous pouvons estimer un ordre de prix pour le renouvellement et installation des postes à hauteur de 15 000€ maximum. Le devis vous sera envoyé après validation et étude de l'inventaire GLPI afin d'être certain d'identifier tous les postes et de faire une commande groupée.

Une formation à l'utilisateur sera mise en place, sur site ou à distance, suivant leur disponibilité. Elle est nécessaire afin de préparer les utilisateurs aux futurs changements de leurs outils informatiques. Les Utilisateurs seront informés par courriels des différentes formations prévues à leur égard.

4. Hot Solution

Le principe est simple : dès que vous avez une question ou un problème, il vous suffit de nous appeler, et vous serez directement mis en relation avec la personne qui saura au mieux vous répondre.

Si votre demande nécessite un exemple visuel ou une résolution rapide, nous pouvons grâce à un logiciel de contrôle à distance prendre la main, avec votre accord, sur votre poste et ainsi vous permettre de travailler à nouveau dans de bonne condition et sans délais de déplacement.

Nous mettons aussi à disposition une boîte mail qui vous est réservé. Elle vous permet de nous envoyer des documents, et d'échanger sur des points à traiter ultérieurement.

Notre but étant de traiter vos demandes efficacement et dans des délais courts, la Hot Solution est le meilleur moyen d'intercommunication possible entre vous et nous.

IV. Documents

1. Mémo interne

A : Techniciens informatiques d'ITP²
De : Directeur Technique
Sujet : Politique d'ITP² concernant la conduite à tenir chez un client
Date : 10/01/2015

L'attitude et l'apparence des techniciens reflètent directement l'image de l'entreprise. Dans un souci de qualité de nos services voici un mémo concernant la conduite à tenir chez le client. Nous serons vigilants aux bonnes applications de ces règles. Le non-respect de celles-ci donnera suite à des sanctions.

-Porter une tenue correcte. Respecter les utilisateurs et rester polis et courtois. Cela va de soi que ces règles s'applique aussi par téléphone.

-Soyez pédagogue ! Les personnes qui utilisent les postes sur lesquels vous intervenez n'ont pas vos qualifications et vos connaissances. Expliquer leurs les problèmes simplement en prenant le temps, ainsi que les solutions à ces derniers.

-Informer les utilisateurs sur ce que avez fait, ce que vous faites et ce que vous allez faire, notamment un point important : La durée d'intervention, c'est-à-dire dans combien de temps l'utilisateur pourra à nouveau utiliser son PC.

- Il est strictement interdit aux techniciens de consulter les documents personnels des clients sans leur autorisation préalable. Le vol de documents confidentiels dans le but de les communiquer à des tiers sera soumis à de lourdes sanctions, autant sur le plan interne que pénal.

-Vérifier que la solution que vous avez utilisé pour traiter le problème est la bonne, et que la panne n'est plus.

2. Plan d'intégration des nouveaux arrivants

L'accueil et l'intégration de nouveaux employés est primordiale. Il est nécessaire que chaque personne soit à l'aise dans son environnement de travail afin de se sentir impliqué.

Nos objectifs sont les suivants :

-Faciliter et favoriser l'intégration sociale et professionnelle de l'employé dans son nouveau milieu de travail.

-Démontrer au nouvel employé la volonté de l'entreprise de l'aider dans son adaptation.

-Permettre à l'employé d'obtenir des réponses à ses interrogations et d'avoir accès à l'information pertinente.

-Soutenir l'employé afin qu'il devienne autonome le plus rapidement possible.

-Communiquer à l'employé les attentes relatives à ses tâches, rôles et responsabilités.

-S'assurer que l'employé connaisse les normes et les politiques de l'entreprise.

-Familiariser l'employé avec la culture et les valeurs de l'entreprise.

-Faire connaître l'entreprise et contribuer au développement de son image.

-Réduire l'anxiété du nouvel employé qui peut être causée par le défi de se familiariser à un nouveau travail, le désir d'être à la hauteur, le besoin d'être accepté par sa nouvelle équipe, etc…

3. Clause de confidentialité nouvel entrant

Clause de confidentialité ITP²

Je soussigné Monsieur/madame : _____, exerçant les fonctions de : _____ au sein de la société IT PROVIDER², étant à ce titre amené à accéder à des données personnel, déclare reconnaître la confidentialité des données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, à prendre toutes précautions conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès et en particulier d'empêcher qu'elles ne soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particuliers à :

- Ne pas utiliser les données auxquelles je peux accéder à des fins autres que celles prévues par mes attributions
- Ne divulguer ces données qu'aux personnes dûment, autorisées, en raison de leurs fonctions, à en recevoir, qu'il s'agisse de personnes privés, publiques, physiques ou morales.
- Ne faire aucune copie de ces données sauf si c'est nécessaire à l'exécution de mes fonctions.
- Prendre toutes les mesures conformes aux usages et à l'état de l'art dans le cadre de mes attributions afin d'éviter l'utilisation détournée ou frauduleuse de ces données
- Prendre toutes précautions conforme aux usages et à l'état de l'art pour préserver la sécurité matérielle de ces données
- M'assurer dans la limite de mes attributions, que seuls des moyens de communications sécurisées seront utilisés pour transférer ses données.
- Assurer dans la limite de mes attributions, l'exercice du droit d'information, d'accès et de rectification de ces données.
- En cas de cessation de mes fonctions restituer intégralement les données informatiques et tout support d'informatique relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera effectif, sans limitation de durée après cessation de mes fonctions, quelle que soit la cause, dès lors que cet engagement concerne l'utilisation et la communication de données à caractère personnel.

J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.

Fait à _____ _____ le __/__/__ en ___ exemplaires.

Nom :
Fonction :
Signature :
Précédée de la mention « lu et approuvé »)

Nom (tuteur) :
Fonction :
Signature :

4. Ticket d'intervention

Voici à titre informatif la procédure utilisé pour traiter vos demandes.

1) Tout commence lorsque vous composez le 04.37.730.730, notre chargé de plateau Hotline Mr. Benssou vous répond.
2) Il prend note de votre demande en complétant un formulaire sur logiciel, renseignant nom, prénom, numéro de téléphone, nom de l'entreprise, numéro de poste, type de demande, son niveau d'urgence ainsi qu'un onglet "description" dans lequel est écrite votre requête.
3) Il envois ensuite le formulaire sous forme de ticket à la personne la plus apte à vous répondre.
4) Cette personne, généralement un technicien informatique, prend connaissance de votre demande et commence dès lors à trouver une solution s'il y n'en a pas déjà une.
5) Selon le type d'intervention le technicien vous répondra par téléphone, ou prendra la main sur votre poste (avec votre accord) pour résoudre le problème.
6) Une fois le problème résolue, le technicien rempli un onglet "solution" en expliquant ce qu'il a fait.
7) Puis un génère, toujours sur le même logiciel, une "ligne de temps" en renseignant le temps d'intervention. (Le temps sera débité sur votre forfait)
8) Le ticket est maintenant prêt à être régler. Une case à coché et le ticket est stocker avec les autres dans "Ticket régler"

GLOSSAIRE (Source : www.hadopi.fr) :

- Active Directoy

Active Directory (AD) est la mise en œuvre par Microsoft des services d'annuaire pour les exploitations Windows. L'objectif principal d'Active Directory est de fournir des services centralisés d'identification et d'authentification à un réseau d'ordinateurs utilisant le système Windows. Il permet également l'attribution et l'application de stratégies, la distribution de logiciels, et l'installation de mises à jour critiques par les administrateurs. Active Directory répertorie les éléments d'un réseau administré tels que les comptes des utilisateurs, les serveurs, les postes de travail, les dossiers partagés, les imprimantes, etc.

- Administrateur

L'administrateur, ou le webmestre ou le webmaster, est la personne en charge de la création et des mises à jour des pages d'un site Web.

- Adresse IP

De l'anglais " Internet Protocol ". L'adresse IP est un identifiant unique qui permet d'identifier chaque entité connectée sur un réseau IP comme internet. Dans sa version 4, quatre octets (chaque octet est usuellement représenté en décimal) séparés par des points (par exemple 255.128.162.01) composent cette empreinte numérique. Dans sa version 6, seize octets groupés par deux (chaque groupe est usuellement représenté en hexadécimal) séparés par des signes deux points (par exemple 2001:3cb8:0000:85b3:0100:0230:ac1f:8001).

Il existe deux types d'adresse IP : dynamique ou fixe. Une IP dynamique est une IP qui change de manière cyclique durant l'abonnement. Une IP fixe est une IP qui reste inchangée durant l'abonnement. Tous les fournisseurs d'accès ne procèdent pas de la même manière. Certains fournisseurs d'accès internet donnent la possibilité à l'abonné de choisir entre une IP fixe ou dynamique. Pour plus de renseignements sur votre adresse IP personnelle, nous vous invitons à contacter votre fournisseur d'accès internet.

- Amende

L'amende est une sanction pécuniaire obligeant le condamné à verser une certaine somme d'argent au Trésor Public après qu'une infraction a été commise.

- Anti-virus

Un anti-virus est un programme chargé de lutter contre les virus informatiques.

- Application

En informatique, une application est un programme qui permet de réaliser une ou plusieurs tâches ou fonctions de manière automatisée. On parle parfois de logiciel applicatif. Les applications s'installent sur un ordinateur ou un téléphone. Il peut s'agir d'outils de bureautique, de gestion de données, de jeux, d'émulateurs, d'indexation d'information, etc.

- Atteinte à la vie privée

L'atteinte à la vie privée est le fait de porter atteinte au droit d'une personne au respect de sa vie privée. Le droit au respect de la vie privée est protégé de façon générale par l'article 9 du code civil. Sa violation peut parfois donner lieu à une action devant le juge pénal (article 226-1 du code pénal).

- Box

La box, ou boîtier de connexion, est un modem multiservices permettant d'accéder à des offres Internet et autres services proposés par les fournisseurs d'accès à internet (télévision, téléphonie, vidéosurveillance…).

- Centre d'appel

Le centre d'appel est une plateforme dédiée à la réception et/ou à l'émission d'appels téléphoniques.

- Charte informatique

La charte informatique est un document interne établissant, en accord avec la législation, les responsabilités des utilisateurs des installations informatiques d'une entreprise, d'une administration, d'une association... Elle établit les règles minimales de courtoisie et de respect d'autrui pour un usage correct des ressources informatiques et des services réseaux. Elle fait également connaître aux utilisateurs les mesures de sécurité adoptées.

- CNIL

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante instituée par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Elle a pour mission de protéger la vie privée et les libertés des citoyens dans un monde numérique. (Source : www.cnil.fr).

- Confidentialité

En sécurité informatique et de l'information, la confidentialité est le caractère réservé d'une information, des données, des contenus et de leur diffusion. Une information confidentielle n'est accessible qu'aux personnes ou entités autorisées.

- Contrefaçon

La contrefaçon est une reproduction et/ou représentation illicite d'une œuvre donnant lieu à des sanctions pénales et civiles. Toute reproduction, représentation ou exploitation d'un objet protégé par un droit de propriété intellectuelle accomplie sans autorisation des titulaires de droits ou de la loi constitue un acte de contrefaçon. La contrefaçon est un délit, puni d'une peine maximale de 3 ans d'emprisonnement et 300 000 euros d'amende.

Copyright

Le copyright désigne le système de protection des œuvres littéraires et artistiques dans les pays anglo-saxons. Il peut dans une certaine mesure être comparé au droit d'auteur français. Il est représenté par le signe © suivi du nom du titulaire du droit d'auteur et de l'année de publication.

- Courrier électronique

Le courrier électronique est une communication de messagerie transmis par internet (Appelé aussi courriel ou, en anglais, mail ou email ou electronic mail). On envoie un courrier électronique à partir d'une d'adresse électronique (ou adresse mail).

- Hébergeur

Un hébergeur est une personne physique ou morale qui assure, même à titre gratuit, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature destinés à être mis à disposition du public sur internet.

- Internet

L'Internet est un réseau mondial associant des ressources de télécommunication et des ordinateurs serveurs et clients, destiné à l'échange de messages électroniques, d'informations multimédias et de fichiers. Il fonctionne en utilisant un protocole commun qui permet l'acheminement de proche en proche de messages découpés en paquets indépendants.

- Licence

La licence est un contrat définissant les conditions d'exploitation et les droits d'utilisation et de modification. La licence peut être propriétaire ou libre.

- Logiciel

De l'anglais " software ". Le logiciel est une série d'instructions interprétables par un ordinateur. Le logiciel peut être un ensemble de fichiers incluant des programmes, un script, des données, un code source ou de la documentation, etc. Le logiciel peut être applicatif (les applications), de base ou système (les utilitaires, les systèmes d'exploitation).

- Moyen de sécurisation

Un moyen de sécurisation est un dispositif permettant de sécuriser un système d'information, établi selon une politique de sécurité. En droit français, le fait, sans motif légitime, de ne pas avoir mis en place un moyen de sécurisation ou d'avoir manqué de vigilance dans la mise en œuvre de ce moyen expose le titulaire de l'accès à internet à une condamnation pour négligence caractérisée.

- NAS

Un serveur de stockage en réseau, également appelé stockage en réseau NAS, boîtier de stockage en réseau ou plus simplement NAS (de l'anglais Network Attached Storage), est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

- Onduleur

Un onduleur est un dispositif d'électronique de puissance permettant de délivrer des tensions et des courants alternatifs à partir d'une source d'énergie électrique délivrant un courant. C'est la fonction inverse d'un redresseur. L'onduleur est un convertisseur statique de type continu/alternatif

- Pare-feu

Le pare-feu (ou firewall en anglais) permet le filtrage et le contrôle des connexions sur un réseau. Cet outil permet notamment de sécuriser les ordinateurs et les réseaux locaux connectés de façon continue à Internet en les protégeant contre les intrusions.

- Pirater, Piratage, Pirate

Pirater est le fait de s'introduire illégalement dans le système d'un ordinateur généralement à l'insu de l'utilisateur pour observer, s'approprier ou détourner ou détruire les données. Internet offre de nombreuses possibilités au pirate : il peut hacker ou cracker un système, un logiciel, un site web, une messagerie, une connexion, un navigateur, un périphérique, une application... et invente de multiples techniques (insertion de lignes de code dans le code source, virus, phishing, spam, ver, cheval de troie, logiciel espion...). Il exploite les failles des systèmes informatiques.

- Proxy

Le proxy est un serveur mandataire qui sert d'interface entre les utilisateurs et Internet. Il assure notamment les fonctions de mémoire cache, de sécurité du réseau local, de filtrage et de l'anonymat. Dans le cadre de la sécurisation des systèmes d'information, de nombreuses entités utilisent un proxy pour autoriser ou non l'accès à certains sites.

- Serveur

Le serveur est un ordinateur dont la fonction principale est d'exécuter des opérations à la demande d'autres ordinateurs, appelés clients. Les requêtes des clients peuvent être des demandes d'espace disque, de base de données, d'accès à des périphériques, de traitements automatisés, de sauvegarde centralisée, etc... Par exemple, un navigateur fait une requête à un serveur HTTP pour afficher une page web.

- Switch

Un switch désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique. Contrairement au concentrateur (ou hub), il fractionne le réseau en domaines de collision indépendants.

- Virus

Un virus informatique est un programme qui infecte l'ordinateur, son " hôte ". Un virus s'insère et se cache dans un autre programme. Lorsque le programme infecté est exécuté (lancé), le virus se duplique pour infecter un autre programme. Il peut se répandre de manière autonome ou lors d'échanges de données numériques par messagerie, par les réseaux, par les clés USB. Les virus exploitent les failles des systèmes et l'ignorance des utilisateurs

- VPN

De l'anglais " Virtual Private Network ". Le VPN, dit aussi réseau privé virtuel, permet un accès direct et sécurisé, créé artificiellement, d'un ordinateur à un autre ou à un réseau local.

Sources

- www.Wikipédia.fr
- www.légifrance.fr
- www.google.fr
- www.cnil.fr
- www.olfeo.com
- www.feral-avocats.com
- www.jurispedia.org
- www.gestiondelapaie.com
- www.itil.fr
- www.itsmf.fr

IT PROVIDER²
24 rue Berjon, Greenopolis
69009 Lyon
04.37.730.730
it.pro2@gmx.com

D E V I S

Référence : 952336
Date : 11/01/2015

AutoConcept

Intitulé: Devis prestation initiale

Quantité	Désignation	Prix unitaire HT	Prix total HT
1	*Synology DiskStation DS213j*	*135.20*	*135.20*
2	*Western Digital WD Red - 4 To*	*130.80*	*261.60*
80	*McAfee VirusScan Entreprise (3mois)*	*4.50*	*288.00*
1	Cisco ASA 5512-X	*1910.40*	*1910.40*
1	Installation serveur et ces services	*160*	*160*
80	Formation utilisateur	*10*	*800*
1	Installation VPN, GLPI, Anti-Spam, FireWall	*160*	*160*

Total Hors Taxe	*3318.4€*
TVA à *20%*	*663.68€*
Total TTC en euros	**3982.08€**

Si ce devis vous convient, veuillez nous le retourner signer précédé de la mention :
"BON POUR ACCORD ET EXECUTION DU DEVIS"
Date : Signature :

Validité du devis : 3 mois
Conditions de règlement : 40% à la commande, le solde à la livraison
Toute somme non payée à sa date d'exigibilité produira de plein droit des intérêts de retard équivalents au triple du taux d'intérêts légal de l'année en cours ainsi que le paiement d'une somme de 40€ due au titre des frais de recouvrement

IT PROVIDER²
24 rue Berjon, Greenopolis
69009 Lyon
04.37.730.730
it.pro2@gmx.com

D E V I S

Référence : 952336
Date : 11/01/2015

AutoConcept

Intitulé: Devis mensuel

Quantité	Désignation	Prix unitaire HT	Prix total HT
1	*Hébergement / liaisons spécialisée*	*400*	*400*
1	*Service maintenance du parc*	*1500*	*1500*
80	*Service assistance*	*60*	*4800*

Total Hors Taxe	*6700€*
TVA à *20%*	*1340€*
Total TTC en euros	**8040€**

Nous restons à votre disposition pour toute information complémentaire.
Cordialement,

Si ce devis vous convient, veuillez nous le retourner signer précédé de la mention :
"BON POUR ACCORD ET EXECUTION DU DEVIS"
Date : Signature :

Validité du devis : 3 mois
Conditions de règlement : 40% à la commande, le solde à la livraison
Toute somme non payée à sa date d'exigibilité produira de plein droit des intérêts de retard équivalents au triple du taux d'intérêts légal de l'année en cours ainsi que le paiement d'une somme de 40€ due au titre des frais de recouvrement

Rapport d'audit

IT Provider² souhaite répondre à votre appel d'offre et ainsi obtenir la gestion de votre parc informatique (70 à 80 postes). Vous souhaitez externaliser les prestations informatiques aujourd'hui exécutées par deux informaticiens en internes. Un des deux informaticiens sera recruté dans notre structure si obtention du contrat. Un audit est nécessaire afin de répondre correctement aux attentes et à l'appel d'offre d'AutoConcept.

- Architecture Réseau

Quel genre d'architecture réseau possédez-vous ?
Possédez-vous un Schéma de l'architecture Réseau ?
Quel genre de switch possédez-vous (L2, L3)?
Sont-ils manageable ?
Possédez-vous le WIFI ?
Quel cryptage de clé utilisez-vous (WEP, WPA ou WPA2)?
Avez-vous recours à un Datacenter ? Lequel ?
Possédez-vous un Possédez-vous un WAN (réseau étendu)?
Réseau serveur ? Un réseau utilisateur ? Un réseau VOIP ?
Possédez-vous un VLAN utilisateurs et/ou serveur ?
Possédez-vous un nom de domaine et un hébergeur du nom de domaine ?
Les serveurs sont-ils dans une salle climatisée ?
Votre salle serveur possède-t-elle un accès sécurisé ?
Possédez-vous une salle qui pourrait héberger un ou des serveurs ?
Avez-vous une politique de sauvegarde ?
Si oui laquelle ?
Seriez-vous ouvert à une nouvelle solution de sauvegarde ?
Utilisez-vous un Stockage NAS ou SAN ?
Utilisez-vous un Branchement ISCI ou fiber channel ?

Comment gérer vous la sécurité la sécurité informatique ?
Utilisez-vous un Antivirus ? si lequel ?
Utilisez-vous un Firewall ? si oui lequel ?
Utilisez-vous un Proxy ?si oui lequel ?
Gardez-vous les logs du proxy pendant un An ?
Utilisez-vous des outils monitoring (logiciels de surveillance système du genre Nagios, Centreon ou Zenos)
Possédez-vous une charte informatique ?

- Les Applications et les postes critique

Existe-t-il des postes de travail dites « critique » ?
Existe-t-il des applications dites « critique » ?
Existe-t-il des applications dites « critique » au changement de version d'OS ?

- Inventaire informatique

Combien d'ordinateurs l'entreprise possède-t-elle (tour, portable, autre)?
Quel OS, Service Pack et spécificités (32/64bits) utilisez-vous ?
Quelle suite bureautique utilisez-vous ?
Est-ce que vos licences sont à jour pour les OS et les logiciels ?
Utilisez-vous des Clients léger ?
Utilisez-vous un TSE (terminal service) ?
Vos ordinateurs sont-ils sous prise ondulée ?groupe électrogène ?
Les personnes qui ont un PC portable, s'en servent ils ailleurs qu'à l'entreprise ?
Avez-vous un moyen de répertorier l'ensemble de votre parc avec les critères ci-dessus ? (GLPI)

- Messagerie informatique

Utilisez-vous une messagerie interne ou externe ?
Quel logiciel ou Web Access utilisez-vous?
Quelle est la capacité moyenne de la messagerie?
Possédez-vous un anti spam ? hébergé ?

- Politique face à internet

Votre firewall est-il paramétré face à internet ?
Possédez-vous un accès VPN externe ? (tunnel ipsec)
Utilisez-vous un filtre via proxy ?
Bloquez-vous certain site web ?
Quel est votre politique face au téléchargement ?

- Utilisation de Téléphone portable d'entreprise / tablette

Quelle marque de téléphone utilisez-vous ?
Utilisez-vous la messagerie sur les téléphones ?
Peut-on accéder au réseau avec les tablettes ?

V. CONCLUSION

La solution que nous vous proposons permet non seulement d'être respectueux des lois informatiques. Mais aussi d'acquérir un système informatique sécurisé.

De plus, l'infogérance vous assure un suivi professionnel, une assistance hotline et le déplacement de techniciens en cas de problème.

Enfin, le suivi qualité de notre société, nous engage à respecter des normes de travail strictes qui vous sont donc garanties.

Dans un même temps, vous noterez que la solution proposée peut être mise en place par une équipe de deux techniciens et d'un ingénieur pendant 3 semaines. Nous limiterons un maximum notre impact sur le réseau lors de l'installation du firewall, proxy, anti-spam et système de sauvegarde.

A noter que pour le renouvèlement des postes l'installation se fera de façon progressive et informé par courriel, ne bloquant chaque utilisateur que pendant une demi-journée.

Nous avions cinq mois pour organiser et réaliser le déménagement de notre entreprise vers le nouveau site et nous pouvons affirmer que si nous validons les devis afin de donner le feu vert aux prestataires, le site sera opérationnel dans les délais. Ce projet aura été une totale réussite, et nous sommes certains que nos choix s'inscrivent dans une politique visionnaire d'évolution future qui permettra un gain de temps et d'argent pour l'extension au sein de l'entreprise.