PROJET SAS

Société Jcube

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

VIALATTE Jérémy

LACOTTE Justine

BONIFACE Joffrey

Sommaire

Présentation de l'entreprise Jcube

Jcube est une entreprise informatique créée en 2010 par Mr Boniface, Mlle Lacotte et Mr Vialatte. Son siège social est basé au 16 avenue du Jeandron, 33160 Saint Medard en Jalles. Elle emploie actuellement une vingtaine de personnes, trois directeurs associés, quatre commerciaux, dix technicien informatique, trois assistantes ainsi qu'une secrétaire.

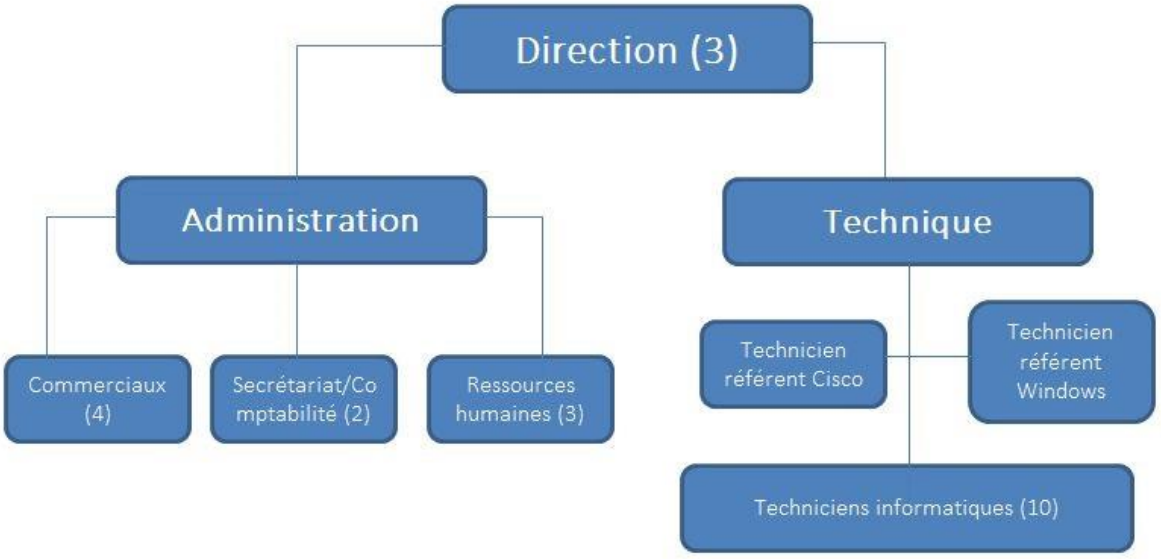
Jcube est spécialisé dans les services informatiques et dans la gestion des infrastructures, des applications ainsi que dans le conseil en technologies.

Jcube est une entreprise qui se veut locale, nous proposons à nos clients des solutions simples, pratiques, pertinente, sur-mesure et innovantes. Sur le territoire Aquitain, J3 accompagne ces clients, grâce à une organisation de proximité réactive.

J3 Informatique 2008

Adresse :
16 avenue du Jeandron
33160 Saint-Medard-en-Jalles
N°Siret :
354 010 000 12345
Telephone :
06.21.34.08.24
Email :

Organigramme de l'entreprise Jcube



Partenaires

CISCO

Prestataire équipement d'infrastructure réseaux informatique professionnelle

VMWARE

Prestataire de logicielle liés à la virtualisation professionnelle

MICROSOFT

Prestataire de systèmes d'exploitation et de logiciels

DELL

Prestataire d'équipement informatique et constructeur

Présentation de l'entreprise AutoConcept

La société **Auto Concept** rassemble 83 salariés, C'est une entreprise spécialisée dans le commerce automobile située au 162 Route De Toulouse à Begles.

Cette société propose un service d'achat, de vente, reprise de véhicules neufs et d'occasions multimarques.

Auto Concept propose également un service de réparation et d'entretien automobile afin que le nouvel acquéreur parte l'esprit léger.

Le nombre de poste informatique s'élève à 66 postes de bureaux et 4 postes portables ainsi que l'équipement réseaux qui est composé d'un server, de deux switches.

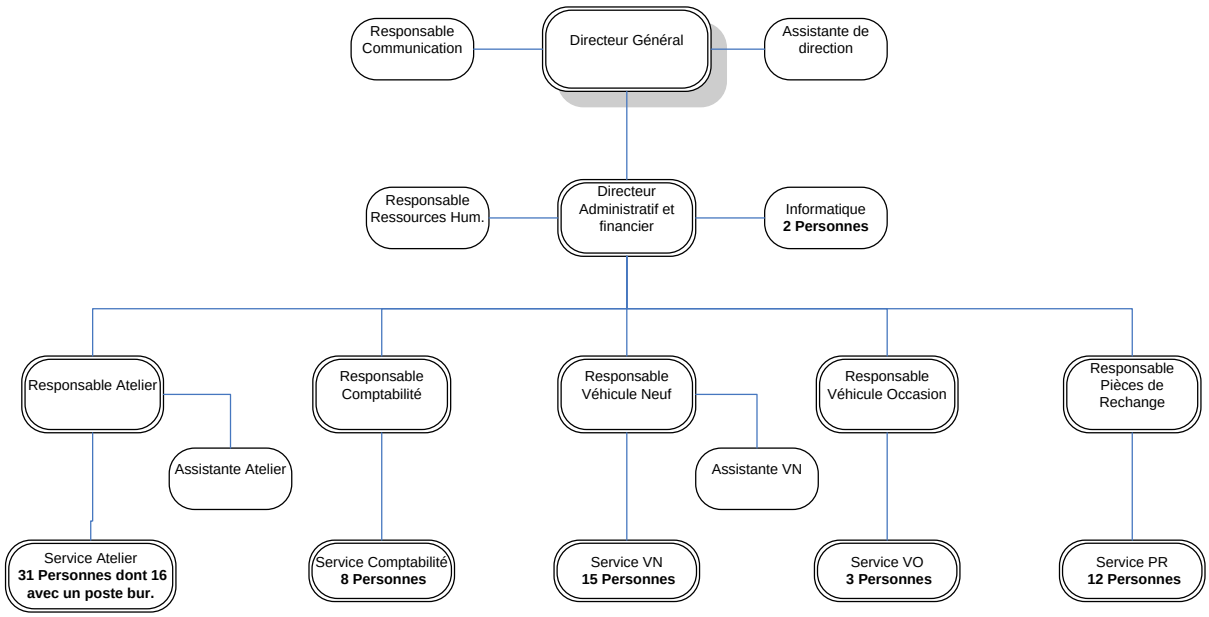
Un appel d'offre a été émis, car la société souhaite déléguer la gestion de son parc informatique suite à divers disfonctionnements au sein de celle-ci.

La société, au fil du temps, c'est confronté à plusieurs obstacles qui ont ralenti son avancée et fait perdre énormément de temps et d'argent. Les derniers soucis en date relaté dans l'appel d'offre nous apprennent que la société a eu des soucis au niveau de la communication envers les informaticiens, la disponibilité des postes et le savoir être des intervenants chez eux.

Au vu des éléments que nous a fourni la société **Auto Concept**, nous nous engageons à vous fournir une solution sur mesure pour subvenir au mieux à vos besoins :

- Introduire une notion de confiance envers un Service Informatique gérer dans les règles de l'art.
- Proposer une solution de gérance de parc informatique simple, sécuritaire et efficace.

Organigramme de la société AutoConcept



L’outil informatique en entreprise

Les nouvelles technologies et plus particulièrement celles relatives à l'informatique, sont de plus en plus présentes dans le monde du travail. Les entreprises quels que soient leur secteur et domaines d’activités on recoure à des Système d’information (SI) de plus en plus sophistiqué. Les employés qui utilisent ces réseaux ont un accès direct avec l’extérieur par le biais d’internet, de la messagerie professionnelles ou tout autre système de communication extérieur. Dans tous les entreprise la sécurité des données est très importante pour éviter une perte du a la divulgation d’information confidentiel. Les utilisateurs qui ont un accès à ce système d’information s’engage par le biais d’une charte informatique et de confidentialité dans certain cas.

Si l’utilisation de l’outil informatique et internet dans l’entreprise est indispensable, pour éviter de mettre en danger l’utilisateur et engager directement la responsabilité de l’employeur. Pour prévenir les litiges, la Commission nationale de l'informatique et des libertés (CNIL) recommande à l'employeur de fixer les limites de l'utilisation, par ses salariés, des outils informatiques qui sont mis à leur disposition pour les besoins de leur activité professionnelle, en respectant des règles.

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.

Dans une première partie nous avons établi une charte d'usage du Système d'information une charte de confidentialité pour votre entreprise. Puis, nous l'avons déterminé les moyens légaux à mettre en œuvre pour la sécurité des fichiers. Nous l'avons ensuite étudié les informations devant être portées aux personnes dans l'entreprise concernant l'utilisation de l'outil informatique. Enfin, nous nous sommes intéressés aux dispositions légales concernant la mise en place d'une solution de filtrage de contenu en entreprise.

Règlement informatique :

Les Principes d'utilisation généraux

L'utilisation des ressources informatique et du réseau pour y accéder sont réserves à l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement sur le réseau sont en outre soumises à l'autorisation par le directeur de l'établissement sur avis consultatif du DSI. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisations prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

Le directeur d'établissement pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : (Carte à puce d'accès ou d'authentification, filtrage d'accès sécurisé …)

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

Conditions de confidentialité

Dans le cadre de son activité l'entreprise récolte et héberge des informations sur sa clientèle et du personnel. L'information se présente sous de multiples formes : stockée sous forme numérique sur des supports informatique, imprimée ou écrite sur papier, imprimée sur films magnétique, transmise par des réseaux informatiques privés ou internet, par la poste, oralement et/ou par téléphone.

La sécurité de l'information est caractérisée comme étant la préservation de :

- Sa disponibilité : L'information doit être accessible à l'utilisateur, quand celui-ci en a besoin.
- Son intégrité : L'information doit être exacte, exhaustive et conservée intacte pendant sa durée de vie.
- Sa confidentialité : L'information doit être accessible qu'aux personnes autorisées à y accéder.
- Sa traçabilité : les systèmes doivent comporter des moyens de preuve sur les accès et opérations effectuées sur l'information.

L'accès par les utilisateurs aux informations et documents conservés sur le système d'information doit être limité à ceux qui leur sont propres, et ceux qui sont propres, et ceux qui sont publics ou partagés. En particulier, il est interdit de prendre connaissance d'informations détenues par d'autres utilisateurs, quand bien même ceux-ci ne les auraient pas explicitement protégées.

Cette règle s'applique également aux conversations privées de type courrier électronique dont l'utilisateur n'est destinataire ni directement, ni en copie pour tout autre moyen de communication d'information protéger par des droits établis par la direction.

Les mesures de protection de l'information s'appliquent également aux documents « papier » lorsqu'ils contiennent des informations confidentielles. Il est conseillé de mettre ces documents sous clé dès que nécessaire, ainsi que d'utiliser un broyer avant de les jeter.

Conditions d'utilisations

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son établissement. L'utilisation de ces ressources doit être rationnelles et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles.

Voire Annexe 1 : Le respect de l'intégrité d'un système informatique.

Chaque utilisateur dispose de compte nominatif lui permettant d'accéder au système d'information de l'entreprise. Pour utiliser ce compte nominatif lui permettant d'accéder au système d'information de l'association. Pour utiliser ce compte nominatif, l'utilisateur dispose d'un login et d'un mot de passe personnel.

Analyse et contrôle de l'utilisation des ressources

L'utilisation des ressources informatiques et du réseau peut donner lieu à surveillance et contrôle à des fins statistiques, de traçabilité, d'optimisation, de sécurité ou de détection des abus. (Utilisation d'outils de métrologie, de filtrage, de scan, de détection de vulnérabilité, de détection d'intrusion, de fichiers de journalisation, d'antivirus, d'anti-spam...)

Ces analyses et contrôles se font dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés, exclusivement par les personnels habilités.

La fourniture d'un accès Internet dans le cadre professionnel oblige légalement à mettre en place un système de journalisation pour conserver les données techniques de connexion (loi du 15 nov. 2001 décret d'application du 24 mars 2006).

Les personnels habilités pour réaliser ces tâches d'administration doivent impérativement respecter la confidentialité des fichiers des utilisateurs.

Voici les règles régissant l'utilisation des moyens informatiques mis à disposition des salariés

Sécurité du système

Le système informatique est une cible sensible. La démocratisation du travail nomade a rendu celui de plus en plus difficile à sécuriser et exposent plus facilement les données critiques de l'entreprise. Pour pallier à ce souci, nous devons former et sensibiliser les utilisateurs aux gestes et reflexes à avoir pour les prévenir des risques pour leurs données s'ils ne suivent pas certaines règles élémentaires de sécurité.

Travailler sur l'humain :

Pour ce faire, nous organiserons des formations, pour faire prendre conscience aux utilisateurs non seulement que le maillon faible de la fuite d'informations se situe le plus souvent à leur niveau, mais surtout qu'avec certains reflexes simples il est possible de diminuer drastiquement ce genre de risque.

Cette formation fera échos à la politique de sécurité que nous prévoyons de mettre en place notamment grâce à une identification unique des utilisateurs, une politique de mot de passe obligatoire pour chaque poste informatique (avec une expiration au bout de 3 mois, une complexité minimum exigée avec une variation du type de caractères et si possible unique pour chaque logiciel utilisé par l'entreprise).

Pour se faire nous donnerons, dans un premier temps, un accès restreint à tous les utilisateurs et attendons des demandes d'accès spécifique en fonction des besoins de chacun. Ces demandes se feront par mail et devront être validés par le supérieur direct.

Anticiper les pertes de données

Afin d'anticiper au mieux les risques de perte de données, nous devons identifier en amont les applications et données sensibles de l'entreprise. Pour ce faire, une fois le devis accepté nous travaillerons directement avec Mr LeDaf ainsi que les chefs de secteur pour identifier précisément les besoins et pouvoir apporter à l'entreprise une aide personnalisé. Une fois cela fait, nous mettrons en œuvre une structure de sauvegarde avec des tests pour vérifier que celle-ci s'effectue bien.
Pour anticiper la perte de donnée nous gérerons aussi toutes les mises à jour des programmes et nos spécialistes effectueront une veille en sécurité informatique. De plus des Audits sur les paramètres sensibles seront régulièrement effectués (une fois tous les 6 mois)

Surveillance réseau

Les intrusions informatiques et la perte de données ont généralement lieu à distance, via le réseau, en réduisant les accès externes au minimum vital a l'entreprise, nous réduisons de par ce fait les risques d'une perte extérieur. Pour une plus ample surveillance, un pare-feu sera installé en entrée dans un premier temps, s'en suivront un logiciel d'analyse des flux sortants de l'entreprise pour pouvoir détecter les tunnels (SSH, HTTPS ou DNS) installés à l'intérieur de l'entreprise par les employés eux même pour pouvoir contourner les filtres. De plus nous installerons un contrôle d'accès 802.1x qui permet d'éviter le raccordement d'équipement sur le réseau non voulu.

Informations fournies à l'administrateur

Pour pouvoir correctement administrer un réseau, il faut que les bonnes informations remontent en premier à l'administrateur. Pour ce faire ce dernier auras accès à une documentation synthétique de suivi pour visualiser l'amélioration du niveau de service (et ainsi pouvoir en rendre compte à Mr LeDaf de l'avancée en termes de sécurité) et par la suite nous pourrons déployer une console qui permettra de bien visualiser toutes les demandes.

Gérer l'utilisation d'internet en entreprise :

Pour pouvoir contrôler le contenu auquel les collaborateurs doivent avoir accès, il nous faut avoir une vision de toutes les ressources dont les personnes ont besoin. Avec ces informations là nous pouvons mettre en place et maitriser le contrôle d'accès et les droits des collaborateurs sur le système informatique.

Selon la CNIL, l'outil internet ne doit pas être restreint au point de bloquer l'accès à toutes les contenue personnel, mais il ne doit pas dépasser un délai raisonnable et ne pas enfreindre les lois ainsi que l'éthique.

Bien entendu les pauses libres (Déjeuner, pause cigarettes) ne peuvent pas être impactées par la restriction de contenu à la condition qu'elles soient faites sur des appareils hors du réseau de l'entreprise.

Pour ce faire, nous créerons une charte informatique donnant la bonne conduite à avoir en ce qui concerne l'usage du matériel informatique mis à la disposition de chaque utilisateur. Elle servira donc de point d'appui en cas de mauvaise utilisation ou utilisation non professionnelle d'internet.

Voici ce que les points les plus importants à retenir et à communiquer à l'utilisateur :

Pratique de protection des ressources

- Avoir un mot de passe personnel, non-générique, répondant à une norme définie et devant être changé régulièrement

- Ne jamais communiquer son identifiant et son mode de passe à une tierce personne (même un collègue) Ne jamais communiquer son identifiant et son mode de passe à une tierce personne (même un collègue)

- Protéger ces documents confidentiels dans un dossier prévue à cet effet sur le serveur (Dossier nominatif dont seul la personne et l'administrateur réseau peuvent avoir accès)

- Ne pas répondre au message type SPAM (Message à caractère publicitaire, hameçonnage…) provenant de l'extérieur de l'entreprise

- Ne pas ouvrir de pièces jointes d'un mail extérieur à l'entreprise sans en connaître l'émetteur

- Ne pas laisser sa session ouverte sans surveillance (même le temps d'une courte pause)

- Ne pas laisser de supports informatiques avec des informations sur l'entreprise à portée de tous (Disques dur externe, clé usb, CD, DVD, Blu Ray, Disquette…)

- Ne pas laisser trainer des documents sur le fax/scanner sur le bureau ou dans les zones communes

Pratique d'utilisation

- L'utilisateur est responsable de l'usage qu'il fait des ressources de l'entreprise. De par ce fait il ne doit se livrer à aucune activité répréhensible par la loi ou nuisible à l'entreprise.

-Ne pas installer de logiciels sans accord préalable de l'entreprise

Traitement et Filtrage des données informatique

Les modalités de la cyber surveillance

Le code du travail prévoit une information et une consultation des institutions représentatives du personnel « sur les moyens ou les techniques permettant un contrôle de l'activité des salariés » ainsi qu'un contrôle concernant « les atteintes aux libertés individuelles ». Les techniques de filtrages doivent être connus des salariés et des représentants du personnel, comme le prévoie le Code du travail, sont le plus souvent légale

La loi du 6 juillet 1978 impose que le traitement automatique des données personnelles soit déclaré à la CNIL. Le contrôle doit être justifié par la nature des taches et proportionné au but recherché. Autrement dit les données contrôlées doivent être concises et utile.

La sécurité physique

Définition : La sécurité physique vise à favoriser l'exploitation des équipements informatiques dans des conditions fonctionnelles optimales, de manière à bénéficier d'un maximum de performances durant un maximum de temps.

Les installations informatiques peuvent subir différents types de dégâts, dans ceux-ci on peut trouver :

- Dégâts des eaux
- Dégâts du feu
- Défaillance de la climatisation
- Dégradations par des rongeurs
- Problèmes sur le réseau électrique
- Problèmes électrostatiques
- Dégât causés par une tierce personne

Prévenir les risques pour mieux les gérer :

• Dégâts des eaux : ceux-ci peut être causés par une rupture de canalisation, une infiltration d'eau due à une défaillance du bâtiment ou des pluies trop importantes. Pour remédier à ce souci nous utilisons des systèmes de détection de fuite, une isolation des plus complète des câbles d'alimentation et le matériel devra être surélevé.

• Dégâts du feu : celui-ci peut être causés par un incendie criminel ou accidentel ou un disfonctionnement électrique. Pour remédier à ces soucis nous mettrons en place un système d'extinction de feu qui préserve l'ensemble de notre matériel informatique ainsi que l'interdiction de stocker du matériel inflammable dans cette pièce.

• Défaillance de la climatisation : celui-ci peut être causé par de multiple sources, pour nous prévenir de tout problème nous installerons un système d'ouverture de la salle ainsi qu'un système de contrôle de la température dans la salle.

• Dégâts liées aux rongeurs : peut-être causé par une mauvaise isolation de la pièce, pour nous prévenir de ce genre de problème nous utiliserons un appareil a ultrason qui éloigne les rongeurs.

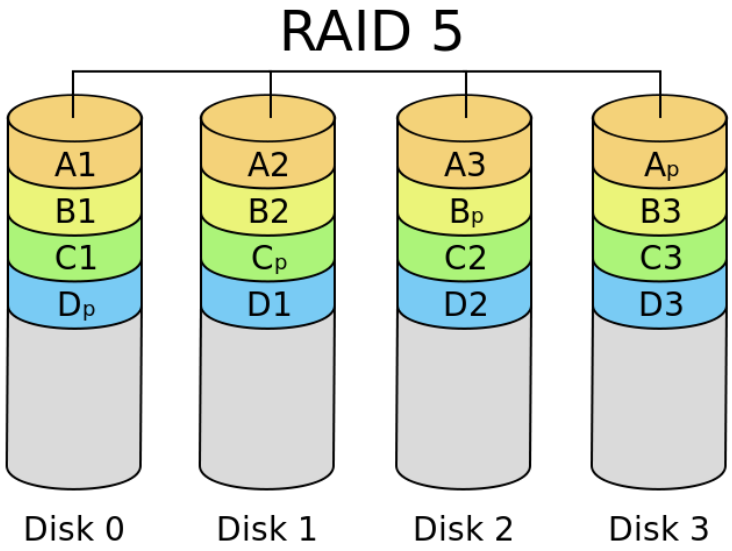
• Dégât liée au réseau électrique : ceux-ci sont causé par une sous tension, une sur tension ou une coupure d'électricité. Pour pallier à ces soucis nous installerons des onduleurs permettant un arrêt propre des serveurs.

• Problèmes électrostatiques : ceux-ci sont causés par des conditions météorologiques particulières ou d'autres objets a fort rayonnement électrostatique. Pour pallier à ces soucis nous instaurerons un port de bracelet de mise à la terre lors de toutes les interventions.

• Dégât causés par une tierce personne : pour pallier à ce souci, seules les personnes habilitées seront aptes à accéder à la salle serveur. De par ce fait toutes intervention externe doit être faites sous surveillance d'une personne habilité.

Mesure de sauvegarde

Après étude nous avons cherché la solution la plus sure pour éviter à la société AutoConcept une nouvelle perte de données. Pour ce faire, une sauvegarde sur nos serveurs en NAS monté en RAID5 (comme le schéma ci-dessous le montre) en physique sera effectuée de manière journalière et hebdomadaire. Tout ceci sera organisé par notre technicien sur place.



De plus, une deuxième sécurité sera mise en place avec une solution de virtualisation de vos données vers l'extérieur sera appliquée, pour cela nous avons choisi de travailler en collaboration avec Acronis.

Ces 2 solutions apporte une solution à vos problèmes de sécurités sûre et efficace et permettra à vos commerciaux utilisant les accès à distance, via leur pc portable, de sauvegarder leurs données aussi facilement que les utilisateurs de poste fixe.

Charte qualité service client

La cohérence : Nous assurons que l'ensemble des logiciels soie cohérent pour l'utilisation demandé

La confidentialité : Nous assurons le respect de la confidentialité aussi bien par nous que pas nos intervenants. La confidentialité est primordiale pour nous et est assuré.

La sûreté : Nous nous engageons à fournir un système informatique sûr et une exploitation facile à nos clients

L'évolutivité : Nous nous engageons assurer l'évolution de nos systèmes en fonction de l'avancement technologique et pour répondre aussi aux obligations légales.

Les services : Nous proposons un panel étendu de service, comprenant différentes prestations comprenant la mise en service, la maintenance, le suivi et la formation utilisateur.

Le contrôle qualité : Nous mettons en place un service basé sur la qualité et le respect des personnes chez qui nous intervenons. Nous nous engageons à nous améliorer en permanence grâce à un suivi de satisfaction client.

Le respect de l'environnement : Nous nous engageons à mettre en place tous les moyens nécessaires pour la gestion de l'environnement. Pour ce faire nous respectons les normes de tri et de recyclage, la norme IS 14001 ainsi nous fournissons aussi un bilan énergétique du parc informatique.

Plan de sécurisation des données :

Plan de sécurité :

Introduction d'un technicien Jcube chez AutoConcept :

Pour pouvoir gérer aux mieux les données et pouvoir intervenir au plus vite, un technicien devra être en poste chez Auto Concept. Si le technicien actuellement en place désire rester, il sera intégré à J3, ce qui nous assurera son professionnalisme ainsi que son sérieux tout en nous permettant de vous apporter le meilleur de notre entreprise chez vous. Il aura comme mission la

maintenance directe du parc, la gestion du réseau informatique et pourra être nommé CIL au sein de la société.

Mise à niveau du système :

Avant de mettre en place un plan de sécurité nous devons mettre à niveau, à la vue des soucis rencontré par Auto Concept, le système. Cette mise à niveau se déroulera en deux parties :

1) Mise à jour des licences Windows périmés

2) Mise en place d'une protection virale

Sécurité Logique :

Le technicien présent sur le site devra gérer les droits d'accès aux utilisateurs

Ces droits qui auront été au préalable vu avec Mr LeDaf ainsi que les chefs de secteur.

À la vue des besoins d'Auto Concept, nous mettons aussi en place une politique rigoureuse de mot de passe, ceux-ci seront, suites aux recommandations de la CNIL, constitué d'une majuscule, d'une minuscule, de caractères spéciaux ainsi que de chiffres. Ils devront aussi contenir une longueur minimum de 8 lettres. Ils devront être renouvelées tous les 3 mois et le nombre maximum de tentative de connexion infructueuse est de 6 au-delà le compte est bloqué et l'utilisateur doit faire appel au technicien présent sur place. Ces mots de passe sont strictement personnel et ne doivent être communiqué à personne, pas même au technicien sur place.

Lors de la première utilisation, un mot de passe générique sera donné à l'utilisateur, il sera obligé de le changer pour accéder au bureau ainsi qu'a tous les logiciel métier dont il a besoin.

Memo Interne

A tous les collaborateurs,

En vue de notre future collaboration avec la société AutoConcept, et après lecture du cahier des charges, il nous a paru important de faire un rappel de quelques règles à suivre, vis-à-vis de notre client.

En général :

• Tenue vestimentaire adaptée au règlement de l'entreprise

• Pensez à faire un bon usage de vos E.P.I (Équipements de Protection Individuelle)

• Soyez courtois et respectueux avec le client au même titre qu'avec vos collègues que ce soit durant le temps de travail ou durant les pauses

Interventions chez un client.

• Avoir une attitude respectueuse, polie et souriante lors de la présence d'un utilisateur ou dans le cadre d'une conversation téléphonique.

• Ne jamais dénigrer un collègue ou votre hiérarchie en présence d'un utilisateur.

• Toujours être à l'écoute du client et lui apporter une solution adaptée à son besoin.

• N'hésitez pas à conseiller les utilisateurs sur l'utilisation de leur poste de travail ou à le sensibiliser à la politique sécurité lorsque vous le jugez nécessaire

• Avoir un langage technique adapté au niveau de chaque utilisateur auprès duquel vous intervenez

• Vous devez être ponctuel et respecter les dates d'intervention. En cas de retard à un rendez-vous chez un client, prévenez-le pour lui donner une heure prévisionnelle de votre arrivée et si besoin reprogrammé une intervention un autre jour.

• Faites remonter toute anomalie que vous pourriez constater sur le poste d'un utilisateur (exemple : licence de logiciel ou logiciel avec licence pirate)

• Donnez des explications rapides à l'utilisateur sur les manipulations que vous effectuez sur son poste.

• Demandez l'autorisation à l'utilisateur avant de faire de quelconques essais avec ces fichiers

• Communiquez un numéro d'intervention à l'utilisateur et le tenir informer de l'avancement de son traitement, en particulier lors d'un retour en maintenance du matériel

• Pensez à bien faire signer la fiche d'intervention par l'utilisateur afin de justifier la clôture de l'incident.

• Respectez les procédures de chaque procédure et faites remonter la moindre erreur constatée

Données et sécurité

• Il est strictement interdit de divulguer toute information ou donnée confidentielle que vous avez été amené à observer, que ce soit à l'intérieur ou à l'extérieur des locaux du client ou sur les postes des utilisateurs.

• Vous ne devez pas installer de logiciel quel qu'il soit sans licence

• Si vous trouvez des données illégales (exemples : pédopornographie, terrorisme…) vous êtes dans l'obligation de faire remonter l'information à votre hiérarchie, afin d'avertir les autorités compétentes.

• Vous n'avez pas à explorer

Annexe 1 : Rappel des lois

Il est rappelé que toute personne sur le sol français doit respecter la législation française y compris dans le domaine de la sécurité informatique :

La protection des libertés individuelles

La création de tout fichier contenant des informations nominatives doit faire l'objet d'une demande préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL). La loi 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et sa loi modificatrice 2004-801 du 6 août 2004 peuvent être trouvées sur le site

La Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) s'applique plus spécifiquement au traitement des données à caractère personnel dans le secteur des télécommunications.

Le respect du droit de propriété

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quel qu'usage que ce soit. Les copies de sauvegarde sont les seules exceptions.

La copie d'un logiciel constitue le délit de contrefaçon sanctionné pénalement (code de la propriété intellectuelle). L'auteur d'une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux répressifs et civils, la personne morale qui l'emploie.

Le respect de l'intégrité d'un système informatique

L'utilisateur s'engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau, à l'intégrité de l'outil informatique et aux relations internes et externes de l'établissement.

La simple accession à un système sans autorisation constitue un délit, même s'il n'en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées.

Il est à souligner que de tels actes (même de simples tentatives) sont susceptibles d'entraîner l'éviction de la fonction publique.

La répression des atteintes aux systèmes de traitement automatisé de données est prévue par la loi du 5 janvier 1988 (Loi dite "Godfrain", du nom de son initiateur), dont les dispositions ont été reprises, depuis le premier mars 1994, par les articles 323-1 à 323-7 du Nouveau Code Pénal.

Le respect du secret de la correspondance

Les utilisateurs doivent s'abstenir de toute tentative d'intercepter les communications privées, qu'il s'agisse de courrier électronique ou de dialogue direct.

La loi numéro 91-646 du 10 juillet 1991 stipule dans son article 2 : "Le secret des correspondances

émises par la voie des télécommunications est garanti par la loi", sont concernés : le téléphone, le télécopieur, les liaisons informatiques et télématiques.

De lourdes sanctions pénales frappent celui qui porte atteinte au secret de la correspondance

(Articles 226-15 et 432-9 du nouveau code pénal).

Texte de loi

Article 323-1 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004)

Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004) Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004) Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Annexe 2 : Devis

Serveur :	Prix HT€	Unité
Rack Dell APC (NetShelter SX24u 600mm*1070mm)	982.17	1
Poweredge R330 Better	34332.64	1
Dell Smart-UPS 3000VA 2U 230V	1586.04	1
Sauvegarde Cloud:		
Acronis License 4TO + AD	4118	1
Informatique :		
Optiplex 5040 + Dell 22 Monitor E2216H	662.16	16
Système d'exploitation + sécurité :		
Windows 10 Professionel OEM	279	54
Trend Business Security	62	70
Climatiseur :		
Climatiseur Daikin FXTB20C / RXB20C	539	2
Pose du climatiseur	800	1
Main d'œuvre :		
Installation	1100	4
Formation	10000	1
Total HT :	59998.72	

Glossaire

CNIL :

La Commission nationale de l'informatique et des libertés (CNIL) est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'Homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi no 78-17 du 6 janvier 1978 modifiée le 6 août 2004.

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.

RAID : Le RAID est un ensemble de techniques de virtualisation du stockage permettant de répartir des données sur plusieurs disques durs afin d'améliorer soit les performances, soit la sécurité ou la tolérance aux pannes de l'ensemble du ou des systèmes.

Sources

- Légifrance
- Cnil
- Wikipedia
- Dell
- Acronis
- TrendMicro
- Microsoft