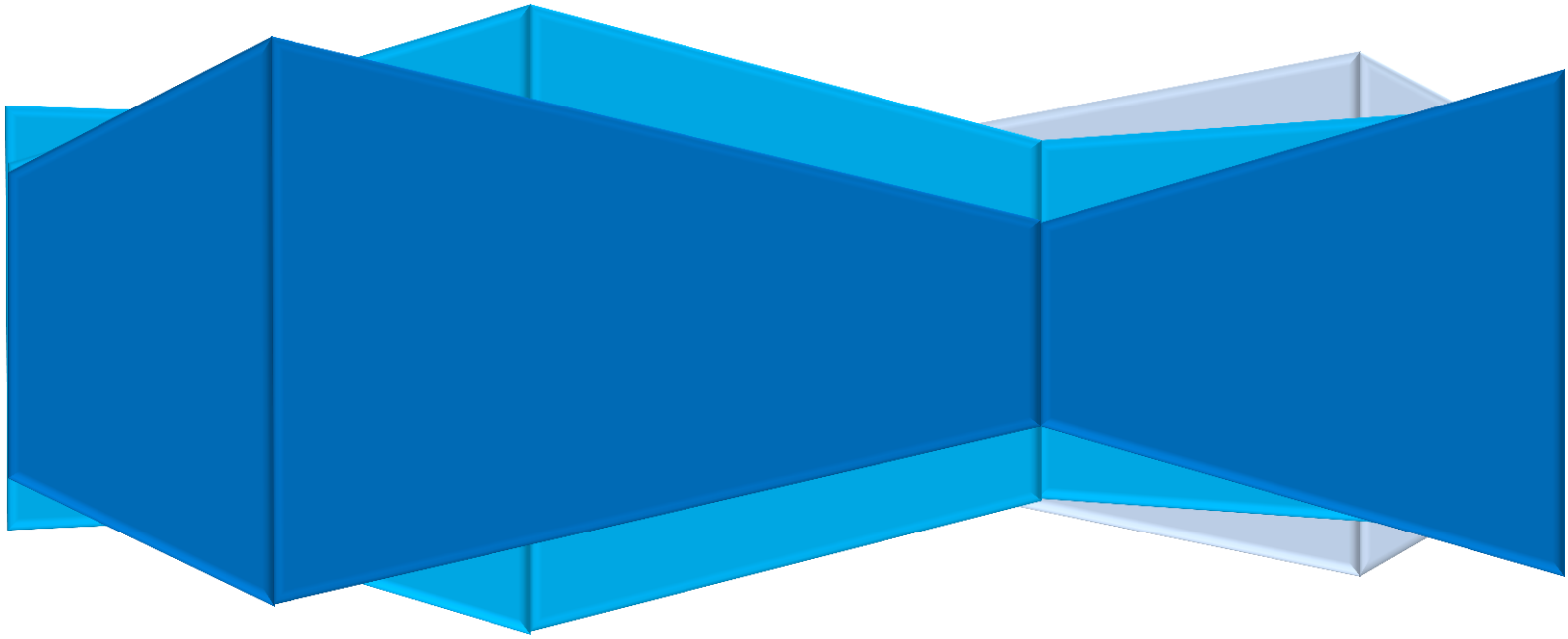
REIPA-INFO

PROJET SAS

GMSI 34

REINE Hugo / PASSETTE Thibault



2012

Sommaire

1) L'entreprise ..... 2 à 4

- Présentation entreprise :

  - Statut entreprise et informations basiques
  - Organigramme
  - Informations complémentaires

2) Présentation du client 5

- Présentation de la société « AutoConcept »
- Organigramme de l'entreprise

3) Charte d'Utilisation ..... 6 à 9

4) Sécurisation des Données ..... 10 à 12

5) Charte Qualité 13

6) Mémo Interne 14

7) Annexes 15

8) Glossaire ..... 16 à 17

Présentation de l'entreprise

REIPA-INFO

REIPA-INFO

Adresse : 18, Rue Thalès - 33700 Mérignac

Ouverture de 8h à 19h du Lundi au Samedi inclus

Téléphone : 09 50 09 50 34

Fax : 09 55 09 50 34

Adresse Mail : contact@reipa-info.fr

Statut juridique: S.A.R.L. (Société à Responsabilités limitées)

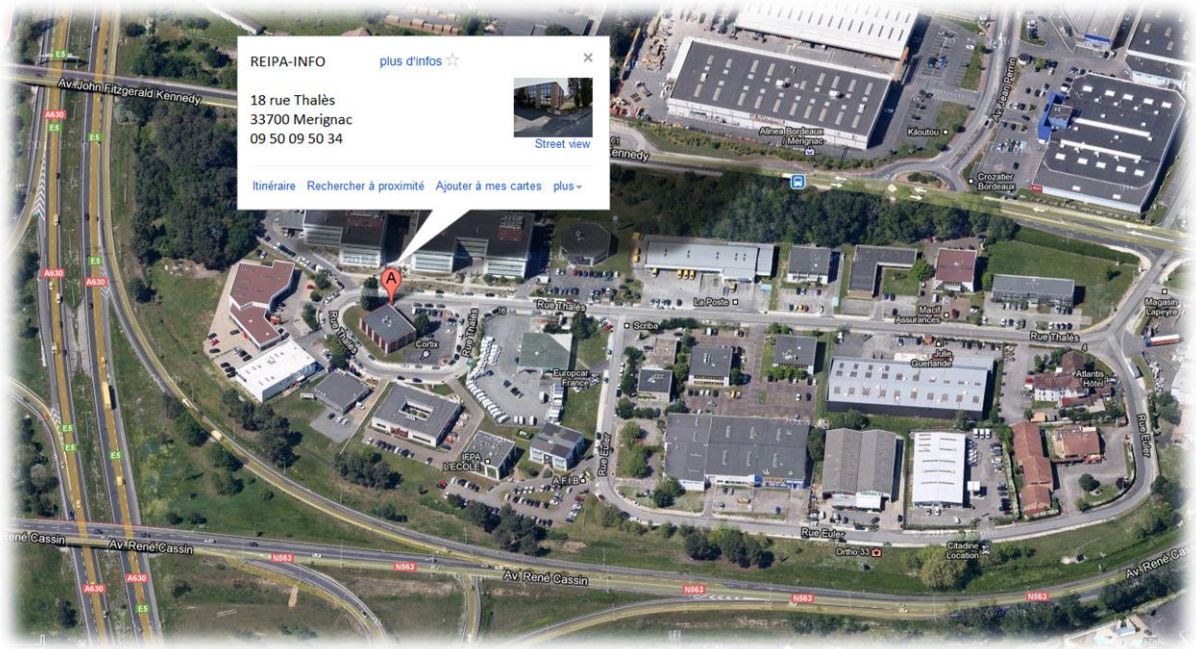
Capital : 14 800€

Responsables de l'entreprise : REINE Hugo et PASSETTE Thibault

Activités principales et Annexes : Installation et maintenance de réseaux et de produits informatiques pour professionnels et particuliers.

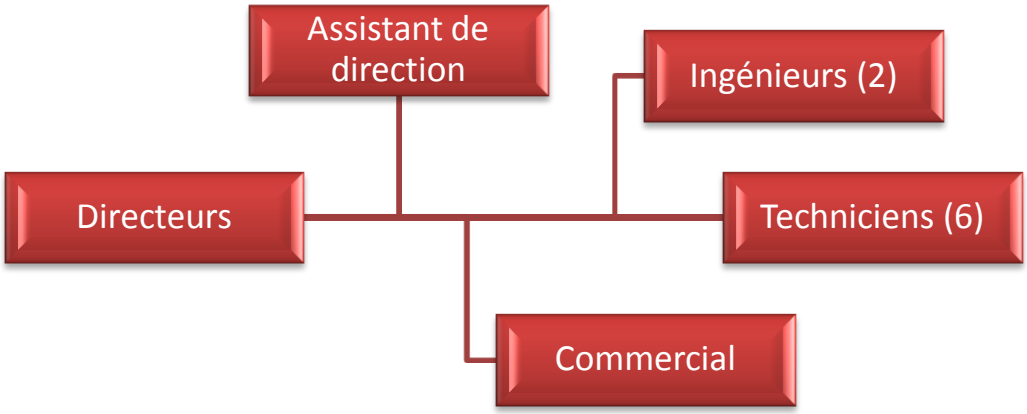
Chiffre d'affaire en 2011 : 850 000€

Effectif de onze personnes.



La société REIPA-INFO est à proximité de la rocade. Elle est d'autant plus visible depuis la mise en place de panneaux publicitaires aux alentours de la rocade et sur l'avenue J.F.Kennedy qui est l'axe routier le plus fréquenté reliant l'aéroport à Mérignac.

- **Organigramme de l'entreprise**



Informations de l'entreprise

- Depuis 2001, REIPA-INFO est présente sur Mérignac.
  Nous proposons aux PME des contrats de maintenance informatique.

- Notre équipe de techniciens disposent de toute l'expérience pour assurer la gestion de réseaux de PME.
  L'équipe informatique est également constituée d'ingénieurs qui assurent le bon fonctionnement des serveurs et applications non dédiées aux techniciens.

  Toute l'équipe est, depuis 2010, certifiée par Microsoft (MCITP).
  Cette certification est accessible uniquement à des personnes ayant au moins deux années d'expérience en tant que professionnel de l'informatique.

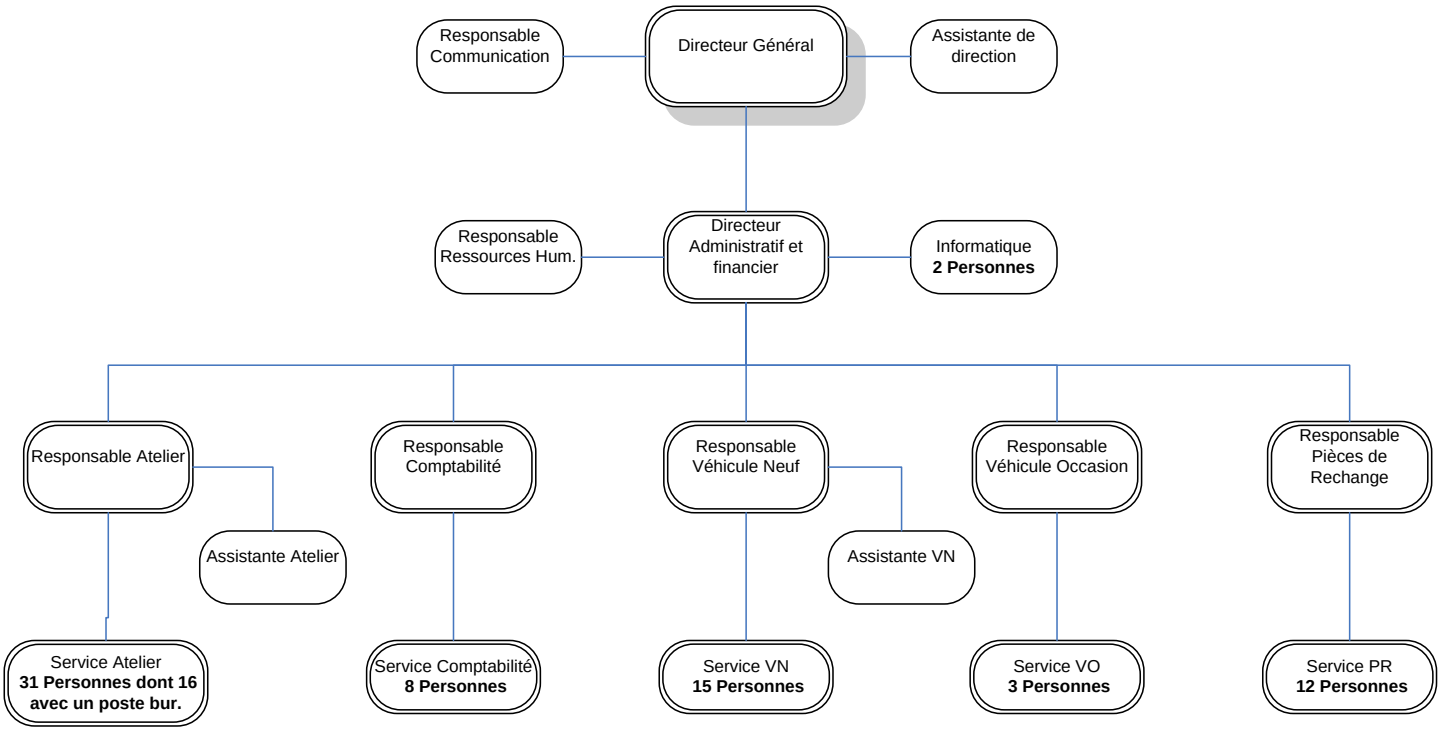
NOS COMPETENCES SONT VOS SOLUTIONS

Présentation du client

Auto Concept

La société **AutoConcept** est un concessionnaire automobile équipée d'un parc informatique de 80 postes.

Voici l'organigramme de la société.



Charte d'utilisation

REIPA-INFO

Définition.

Cette Charte d'Utilisation pour l'usage des ressources informatiques d'AutoConcept a pour objectifs de définir les conditions d'utilisation et les règles de bon usage des ressources informatiques de la société AutoConcept. Elle permet de définir les conditions équitables dans les rapports entre les employeurs et les employés, un équilibre prioritaire pour la pérennité de l'organisation de travail au sein de la société. L'entreprise AutoConcept met en œuvre un système d'information et de communication efficace et nécessaire à son activité, disposant d'un réseau informatique et téléphonique performants. Chaque salarié, dans l'exercice de ses fonctions, est conduit à utiliser les différents moyens de communication mis à leur disposition exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Dans un but d'informations accessibles à tous les utilisateurs du réseau informatique, de règles d'utilisations compréhensibles pour chacun, responsable et sécurisée du système d'information, la présente charte détaille les règles à suivre lors de l'utilisation des ressources sur le réseau, elle permet de trouver le meilleur équilibre entre la sécurité et la liberté d'utilisation des ressources informatiques. Toute personne signant cette charte accepte chaque condition qui la compose et se voit être dans l'obligation de les suivre sous peine de sanction.

Champ d'application.

La présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit son statut dans la société, y compris les salariés, intérimaires, stagiaires, employés de sociétés prestataires. Chaque salarié doit veiller à ce que chaque personne pouvant accéder au système d'information et de communication accepte les règles posées dans la présente charte.

Système d'information et de communication.

Le système d'information et de communication de l'entreprise AutoConcept est composé de serveurs, de stations de travail fixes, d'ordinateurs portables, de téléphones portables, d'imprimantes-photocopieurs, de logiciels, de données et bases de données, d'un système de messagerie, intranet, extranet. Pour des raisons de sécurité du réseau, le matériel personnel des salariés qui est connecté au réseau de l'entreprise est considéré comme faisant partie du système d'information et de communication.

- **Conditions générales d'utilisation.**

La société « AutoConcept » ne pourra être tenu responsable des détériorations d'informations ou des manquements commis par un utilisateur qui ne se sera pas conformé à ces règles. Tout manquement aux règles décrites dans cette présente charte, engage la responsabilité personnelle de l'utilisateur, qui en assume entièrement les conséquences. Chaque utilisateur se doit de participer au bon entretien et de veiller au respect du matériel informatique et suivre les consignes suivantes :

- Interdiction de manger ou boire à proximité d'un poste
- Lancer tous les 15 du mois une défragmentation à l'aide des outils système proposé par l'équipe technique informatique
- Supprimer les fichiers temporaires (cookies, historiques) en vidant le cache du navigateur internet tous les 15 jours.
- Accepter chaque Mises à Jour du système d'exploitation lorsqu'elles sont proposées à l'utilisateur.
- Suppression au moins une fois par semaine de tous les courriels reçus ou envoyés définitivement traités.

Le matériel informatique mis à la disposition des salariés de la société AutoConcept est adapté et configuré pour un usage uniquement professionnel. Tous les logiciels nécessaires à l'exécution des différents travaux des utilisateurs sont installés et gérés par l'administrateur du réseau informatique de la société, la gestion des licences d'utilisation est sous sa responsabilité.

Sauf avec un accord préalable de l'administrateur du système informatique, il est interdit :

- d'installer un logiciel ou toute mise à jour (hors système d'exploitation)
- de faire une copie de logiciel utilisant la base de données de la société
- de faire une copie d'une base de données
- de désinstaller tout logiciel présent sur l'ordinateur utilisé
- de divulguer des informations contenues dans une base de données ou d'un dossier

L'utilisateur a la totale interdiction de stocker ou d'envoyer à partir du réseau informatique de la société tout élément illégal, menaçant, diffamatoire, obscène, pornographique ou tout autre élément qui pourrait violer toute loi de quelque juridiction que ce soit. Cette infraction à la politique de l'entreprise peut entrainer une procédure judiciaire envers l'utilisateur.

- **La sécurité du système informatique.**

Le système informatique contient plusieurs bases de données qui ont chacune une importance particulière pour la société. Par ce fait, il est indispensable d'en sécuriser l'accès pour mieux veiller à la confidentialité des fichiers confidentiels. Toute anomalie constatée, susceptible d'affecter la sécurité des ressources du réseau informatiques, doit être signalée à l'administrateur du système informatique de la société. Pour maintenir la sécurité des données, l'utilisateur doit veiller au respect des règles suivantes :

- ne pas prendre le mot de passe d'un autre utilisateur
- verrouiller son ordinateur en cas d'absence
- éteindre son poste en fin de journée de travail
- interdiction de divulguer son mot de passe personnel
- faire analyser avec l'anti-virus lorsque chaque nouveau périphérique est connecté à l'ordinateur

- **Les droits et les devoirs des Administrateurs du réseau.**

Les administrateurs du réseau de la société sont responsables de la qualité du service et s'engagent donc à prendre toute disposition utile pour permettre le bon fonctionnement des ressources informatiques communes. Les administrateurs du réseau d'AutoConcept doivent informer les utilisateurs des interruptions volontaires de service. Ils s'engagent à les minimiser et à choisir les dates les moins pénalisantes pour les utilisateurs.

Les administrateurs peuvent surveiller en détail les sessions de travail d'un utilisateur soupçonné de non-respect de la charte. Ils peuvent, avec ou sans préavis, prendre les dispositions nécessaires à l'encontre d'un utilisateur qui gênerait le bon fonctionnement des ressources informatiques. Ils peuvent effacer ou comprimer, avec ou sans préavis, les fichiers excessifs ou sans lien direct avec une utilisation normale du système informatique. Ils peuvent mettre fin aux sessions de travail restées trop longtemps inactives.

- **Tout administrateur système a le droit :**

- d'accéder aux informations privées à des fins de diagnostic et d'administration du système, en respectant scrupuleusement la confidentialité de ces informations.
- d'établir des procédures de surveillance de toutes les tâches exécutées sur la machine, afin de déceler les violations ou les tentatives de violation de la présente charte, après autorisation de son responsable fonctionnel et en relation avec le correspondant sécurité du réseau...

- **Tout administrateur système a le devoir :**

- d'informer les utilisateurs sur l'étendue des pouvoirs dont lui-même dispose techniquement de par sa fonction.
- d'installer des licences payantes officielles de Windows sur chacun des postes ainsi que les versions officielles des logiciels payants qu'utilisent l'entreprise.
- d'informer les utilisateurs et de les sensibiliser aux problèmes de sécurité informatique inhérents au système, de leur faire connaître les règles de sécurité à respecter, aidé par le correspondant sécurité du réseau.
- de respecter les règles de confidentialité, en limitant l'accès à l'information confidentielle au strict nécessaire et en respectant un "secret professionnel" sur ce point.
- d'informer immédiatement son responsable fonctionnel de toute tentative (fructueuse ou non) d'intrusion sur son système, ou de tout comportement dangereux d'un utilisateur.

- de répondre aux questions des utilisateurs

Filtrage des contenus en entreprise.

- Un système de filtrage et de surveillance des données est mis en place pour permettre l'externalisation des données de l'entreprise et pour assurer une surveillance du contenu.
- Un fichier de journalisation permettra l'enregistrement des activités de chaque utilisateur. Cela permettra aussi de constater si des attaques ont eu lieu et de les analyser et potentiellement de faire en sorte qu'elles ne se reproduisent pas.
- Un pare-feu contrôlera les communications entre les utilisateurs et le réseau de l'entreprise. Il aura pour fonction de faire respecter la politiques de sécurité du réseau, celle-ci définissant quels sont les communications autorisées et interdites.

Les sanctions encourues au manquement de la charte.

L'utilisateur qui contreviendrait aux règles précédemment définies s'expose à son exclusion de son poste dans la société AutoConcept, ainsi qu'aux sanctions et poursuites pénales prévues par les textes législatifs et réglementaires en vigueur.

- Loi n° 78-17 du 6 janvier 1978 dite «Informatique et Libertés».
- Tout utilisateur qui contreviendrait aux règles aux règles précédemment définies peut s'exposer à des poursuites civiles et/ou pénales prévues par les textes en vigueur (articles sur la fraude informatique de 323-1 à 323-7 du code pénal).

Sécurisation des données

REIPA-INFO

Vous trouverez ci-dessous le plan de sécurisation des données mis en place par notre entreprise.

- **Politique de mot de passe des sessions.**

  - Le mot de passe doit comporter au minimum 8 caractères incluant des lettres, un symbole et des chiffres.
  - Un mot de passe provisoire sera donné à l'utilisateur et lors de la première connexion à sa session personnelle, il devra le changé en respectant le code donné précédemment.
  - Un mot de passe de doit pas être écrit sur un document, divulgué à qui que ce soit ou ne doit contenir des indications personnelles (nom, prénom, date de naissance, etc…)
  - Afin d'assurer une sécurisation optimale, le mot de passe devra être changé tous les 3 mois sans pour autant ressemblé au précédent.

- **Sauvegardes immédiates des données.**

  Pour optimiser la sécurisation des données et l'accès aux ordinateurs, il est nécessaire de mettre en place un certain nombre de procédures et de matériels prévus à cet effet.

  - Pour commencer, nous mettrons en place un serveur sur lequel y sera installé un contrôleur de domaine permettant d'administrer les accès et permissions des utilisateurs aux postes informatiques à l'aide d'un identifiant et d'un mot de passe.
  - Ensuite, nous installerons un système RAID 1 qui permettra de prévenir de toute défaillance matérielle et/ou logicielle du serveur. Ce système a pour fonction de dupliquer les données sur deux disques durs de façon simultanée. En cas de problème, le deuxième disque dur prendra le relais sans aucune répercussion pour l'utilisateur.
    Pour la sauvegarde des données, il sera mis en place un disque réseau NAS en RAID 1 pour les mêmes raisons qui ont étaient citées précédemment.
    Les utilisateurs y auront accès par le biais du réseau de l'entreprise.
  - Pour terminer, nous mettrons en place un pare-feu qui servira de « barrière » entre Internet et le réseau de l'entreprise. Il aura pour principale fonction de filtrer les sites Internet indésirables et d'interdire l'accès à ces derniers s'ils ne sont pas dans le cadre du travail au sein de l'entreprise.

Afin d'assurer un maintien électrique de ces installations, nous installerons un onduleur directement branché sur l'armoire électrique afin de prendre le relais lors d'une coupure électrique.

Ces installations seront regroupées dans un local fermé à clé pour éviter toutes intrusions physique extérieures.

Il sera également mis en place un système de climatisation dans ce local permettant de refroidir les différents matériels.

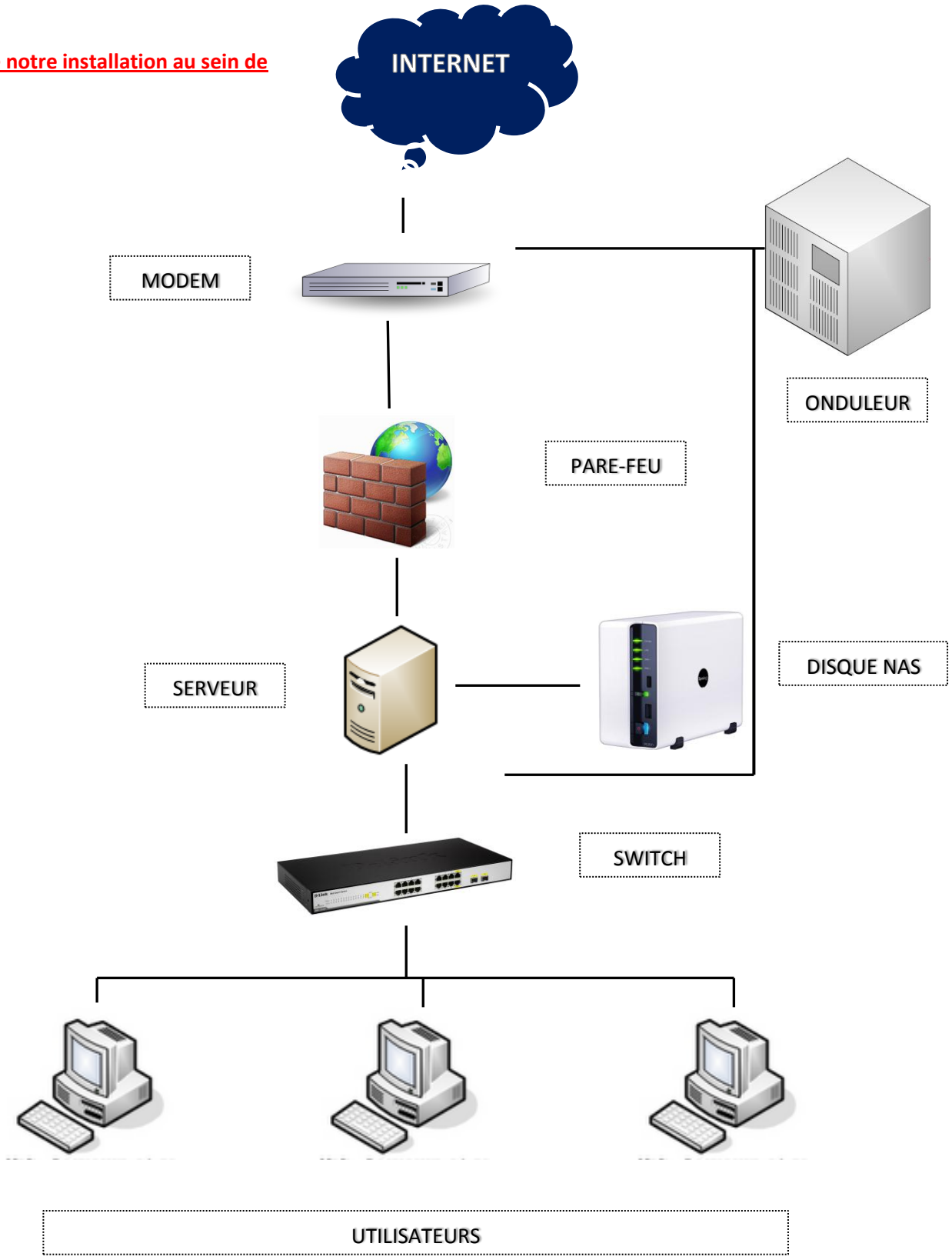
- **Sécurisation des postes.**

Afin de garantir la sécurisation des postes, REIPA-INFO propose l'installation d'un antivirus sur chacun des postes des utilisateurs.
Nous recommandons KASPERSKY Anti-Virus 2013 qui est actuellement le meilleur logiciel contre les virus et les trojans. Pour une meilleure protection, nous proposons à nos clients d'opter pour la version Business Space Security qui offre une protection d'une année pour 10 postes de travail et 1 serveur de sauvegarde de fichiers qui sera appliquée sur le NAS de l'entreprise. Afin de compléter la sécurisation, nous opterons pour la version Work Space Security qui offre une protection d'une année pour 10 postes.

Vous trouverez ci-dessous, un tableau récapitulatif du tarif à l'année pour la sécurisation de l'ensemble des postes.

Version du produit	Quantité	Prix Unitaire	Total à l'année
Business Space Security	*1*	*418 €*	*418 €*
Works Space Security	*7*	*280 €*	*1 960 €*
Total HT			**2 378 €**

Voici le schéma de notre installation au sein de l'entreprise.



Charte qualité

Parce que la qualité de nos services est notre objectif prioritaire, nous avons développé une charte qualité afin de garantir l'entière satisfaction de nos clients.

Ecoute

Notre objectif est de privilégier l'écoute de notre clientèle. Donner des conseils et surtout trouver des solutions pertinentes pour mieux répondre à la demande.

Fiabilité

Offrir un service fiable est une attente légitime de notre clientèle. REIPA-INFO s'engage à privilégier cette démarche au sein de l'entreprise. D'instaurer et d'entretenir un climat de confiance entre vous et nous, REIPA-INFO garantie la gratuité des devis et diagnostics.

Efficacité

De par notre grande expérience, nous nous engageons à être efficace lors de nos prestations et de garantir des solutions en accord avec notre clientèle.

Qualité

REIPA-INFO s'attache à cette notion, auprès de nos collaborateurs et clients, à assurer une qualité de service pour mieux renforcer la notion de fiabilité et de confiance mutuelle. En termes de qualité, nous nous engageons à traiter et à résoudre toutes vos demandes le plus rapidement possible.

Réactivité

REIPA-INFO s'engage à trouver une solution à votre problème dans un délai ne dépassant pas les vingt-quatre heures pour les professionnels et quarante-huit heures pour les particuliers. Si ce délai ne peut être respecté, nous nous engageons à vous fournir une solution de matériel de prêt pour ne pas péjorer le bon fonctionnement de votre société.

Sécurité et confidentialité

Parce que la sécurité et la confidentialité de vos données sont importantes, nous vous garantissons celles de votre entreprise et à ce que vos données soient et restent confidentielles.

Attitude face à la clientèle :

- Tenue vestimentaire correcte exigée
- Utilisation du langage courant dans chaque discussion
- Interdiction de tutoyer le client
- Disposer d'une attitude correcte face au client (ne pas être avachi sur sa chaise)
- Respecter l'interlocuteur
- Etre ponctuel, respect des horaires de l'entreprise et des rendez-vous clientèle
- Se montrer rassurant en utilisant des phrases positives
- Adapter le langage technique selon le niveau de connaissance de l'interlocuteur

Attitude au téléphone :

- Citez le nom de l'entreprise à chaque prise d'appel téléphonique
- Interdiction d'utilisation de mots grossiers lors d'un entretien
- Le débit de parole doit être normal, pour une meilleure compréhension des explications

Attitude en intervention :

- Pour chaque intervention, tenir une fiche de prise en charge matériel (voir annexe page 18).
- Faire un suivi de chaque manipulation effectuée sur le matériel pour la fiche de prise en charge.
- Chaque équipement doit être testé plusieurs heures avant remise en main au client
- Les données « utilisateurs clients » sont bien évidemment privées et ne doivent pas sortir de l'entreprise mais peuvent être vérifiées par le S.A.V.
- Respect du cadre réglementaire. En cas de découverte de données à caractères pédophiles, veuillez en informer immédiatement votre supérieur hiérarchique
- Contactez la hiérarchie en cas de non résolution d'un problème technique ou d'un client mécontent.

Annexes

REIPA-INFO

- **Charte d'Utilisation**

  - Le Journal du Net (http://www.journaldunet.com)
  - Lycée Professionnel François Mitterrand de Château Chinon (http://www.lpfm.fr)
  - Réseau Osiris (http://www.osiris.unistra.fr)
  - Université de La Rochelle (http://www.cri.univ-lr.fr)

- **Sécurisation des Données**

  - Guides CNIL (http://www.cnil.fr/en-savoir-plus/guides)
  - Olfeo (http://www.olfeo.com)
  - Kaspersky (http://boutique.kaspersky.fr/acheter-telecharger-anti-virus-pc-pour-entreprise.html)

- **Charte Qualité**

  - Percy Miller (http://www.percy-miller.com)

- **Mémo Interne**

  - Pas de sources Internet.

- **Autres**

  - Logos (http://www.freelogoservices.com/fr)
  - Bon de prise en charge de matériel (TekMédia)
  - Géolocalisation (Google Maps – Google Earth)

Glossaire

- **Pare-Feu** : Périphérique matériel ou application logicielle conçu(e) pour empêcher les utilisateurs externes au réseau et/ou les applications et fichiers malveillants d'accéder au réseau. Cela permet également de filtrer les sites internet visibles par les utilisateurs par exemple.

- **Modem** : Le modem est un périphérique servant à communiquer avec des utilisateurs distants par l'intermédiaire d'une ligne téléphonique. Il permet par exemple d'échanger (envoi/réception) des fichiers, des fax, de se connecter à Internet, d'échanger des courriels, de téléphoner ou de recevoir la télévision.

- **Routeur** : Son rôle est de faire transiter les informations d'une interface réseau vers une autre, selon un ensemble de règles.

- **Serveur** : Ordinateur qui fournit des services à des clients. Par exemple le stockage de fichier, l'hébergement d'applications ou l'hébergement de sites web.

- **Serveur NAS** : Un serveur NAS, 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.

- **Switch ou commutateur** : Un switch ou commutateur réseau est un équipement qui relie entres eux plusieurs ordinateurs dans un réseau informatique.

- **Onduleur** : Il permet de prendre le relais lors d'une coupure du courant, afin de continuer à alimenter les périphériques qui lui sont rattachés. Cependant fonctionnant sur batterie, il continuera à alimenter les matériels que pendant un certain laps de temps. Ce système permet par exemple de sauvegarder un document en cours ou d'éteindre un serveur correctement.

- **Système d'exploitation** : C'est l'ensemble de programmes d'un appareil informatique qui sert d'interface entre le matériel et les logiciels applicatifs.

- **R.A.I.D**: *Redundant array of independent/inexpensive disks*. Système de sécurité contre les pannes de disques durs.

- **C.N.I.L** : La ***C****ommission* ***N****ationale de l'****I****nformatique et des* ***L****ibertés* 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

- **Dispositif de filtrage** : C'est un système permettant par exemple de choisir les sites internet interdits aux utilisateurs ou d'interdire l'accès à des forums ou chat.

- **Domaine** : Il reflète le plus souvent une organisation hiérarchique dans une entreprise. Par exemple, le domaine "COMPTABILITE" désigne l'ensemble des machines réseau (stations, imprimantes, ...) du service Comptabilité, et les comptes utilisateurs qui sont autorisés à s'y connecter. Il se peut également qu'il englobe la totalité des comptes utilisateurs de la société.

- **Contrôleur de domaine** : Il permet à l'administrateur réseau de gérer plus efficacement les permissions faites aux utilisateurs des stations déployées au sein de l'entreprise car toutes ces informations sont centralisées dans une même base de données. Cela permet de sécuriser le réseau plus efficacement.

- **Base de données** : C'est un lot d'informations stockées dans un dispositif informatique utilisé par des applications.

- **Antivirus :** Les antivirus sont des logiciels conçus pour identifier, neutraliser et éliminer des logiciels malveillants (dont les virus ne sont qu'un exemple). Ceux-ci peuvent se baser sur l'exploitation de failles de sécurité, mais il peut également s'agir de programmes modifiant ou supprimant des fichiers.

- **Virus** : Un virus informatique est un logiciel malveillant conçu pour se propager à d'autres ordinateurs en s'insérant dans des logiciels légitimes, appelés « hôtes ». Il peut perturber plus ou moins gravement le fonctionnement de l'ordinateur infecté. Il peut se répandre à travers tout moyen d'échange de données numériques comme les réseaux informatiques et les cédéroms, les clefs USB, etc.

- **Trojan :** Les trojans sont programmés pour être installés de manière invisible, notamment pour corrompre l'ordinateur hôte. La principale différence entre les virus, les vers et les chevaux de Troie est que ces derniers ne se répliquent pas.

Bon de prise en charge Matériel

REIPA-INFO

18 Rue Thalès
33700 Mérignac
Tél: 09-50-09-50-34
Fax: 09-55-09-50-34
Contact@reipa-info.fr

Client

Date de prise en charge: | Pris en charge par : Romain

Nom / Prénom: | Société:

Adresse : | Code postal:

Ville:

Portable: | Téléphone: | Adresse mail:

Identification du Matériel

Type de matériel: Portable | Marque: | Modèle

N° de série: | Utilisateur / Mot de passe:

Matériel laissé : ☐ Sacoche ☐ Alimentation ☐ Autres : Préciser :

Motif de la panne et tests effectués	
Diagnostic Travaux effectués Remarques	

Nos dépannages matériels sont garantis 3 mois, pièce et main d'oeuvre, sauf dommages accidentels.
Pour éviter les abus, aucune garantie ne sera applicable aux dépannages logiciels.

☐ Devis validé par le client
☐ Pièce commandée / attente réception
☐ Matériel à rendre au client / Facture établie

REIPA-INFO

" Nos compétences sont vos solutions "

Accord préalable.

Responsabilité :
J'ai conscience que mon portable pourra être démonté, annulant ainsi toute garantie constructeur. Je confie mon portable en l'état et déclare assumer tout dégât éventuel conséquent au démontage / remontage de mon ordinateur.
J'ai bien noté que la sauvegarde des données est sous ma seule responsabilité et déclare avoir pris les dispositions nécessaires.
Bon pour accord de prise en charge aux conditions définies ci-dessus ou après acceptation du devis qui me sera adressé préalablement à l'intervention.

Nom du signataire :

Signature :

La signature de ce formulaire implique de plein droit l'acceptation des conditions définies ci-dessus et vaut accord préalable.

Imprimer le formulaire