

PROJET SaS

SOMMAIRE

I.	<u>Présentation du projet SaS</u>	3
II.	<u>Objectif du projet</u>	3
III.	<u>Présentation de l'entreprise</u>	4
	a. Fiche d'identité	4
	b. Historique de l'entreprise	5
IV.	<u>Présentation du client</u>	6
V.	<u>Note de Synthèse</u>	7
	a. Introduction à la sécurité d'un système informatique	7
	b. La sécurité des fichiers	8
	c. Informations à porter aux utilisateurs	9
	d. Les dispositions légales pour le filtrage des contenus	10
VI.	<u>Sauvegarde/stockage des données sur serveur</u>	11
VII.	<u>Conclusion</u>	12
VIII.	<u>Annexes</u>	14

I. Présentation du projet SaS

Notre entreprise **MATI** est une SARL. Le projet SaS consiste à répondre à un appel d'offre pour la gestion du système informatique de l'entreprise **AutoConcept**.

AutoConcept souhaiterait externaliser les prestations informatiques. Le directeur de *MATI* nous charge de réaliser une partie de l'étude avant-vente. En cas d'obtention du marché, un des deux techniciens qui s'occupaient du système informatique sera recruté au sein de notre entreprise. Nous serons donc chargés de son accueil et de son accompagnement.

Nous devons pour cela suivre le cahier des charges et de ce fait atteindre l'ensemble de ces objectifs.

II. Objectif du projet

Le projet SaS a été mis en place pour satisfaire les demandes des entreprises collaboratrices en matière de comportement de ses nouveaux salariés.

- Acquérir les comportements appropriés en entreprise.
- Identifier les mesures réglementaires régissant la mise en œuvre de l'informatique dans l'entreprise.
- Être capable d'apporter des solutions rapides à des problématiques perturbant le bon fonctionnement de l'entreprise dans sa production de biens ou de services.
- Être capable de concevoir un dossier de synthèse, de communiquer et défendre les choix effectués.

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

III. Présentation de l'entreprise

a. Fiche d'identité

Adresse :

18 avenue de la Paix
92 000 Nanterre (France)

Téléphone :

+33(0)5588770000

Fax :

+33(0)5588770001

E-mail :

contact@mati-informatique.com

N° SIRET :

123 123 123 1234561

Chiffre d'affaires :

175 000€

Capital Social :

7 500€

Secteur d'activité :

Informatique, Réseau, Périphérique, Gestion.

Nombre d'employés :

Le Directeur, l'Assistante et quatre techniciens.

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

b. Historique de l'entreprise

L'entreprise fut créée en 2001 par Mr PIGNER dans la ville de Nanterre.

Elle a débuté son activité uniquement avec le particulier, pour ensuite s'attaqué aux petites puis grandes entreprises.

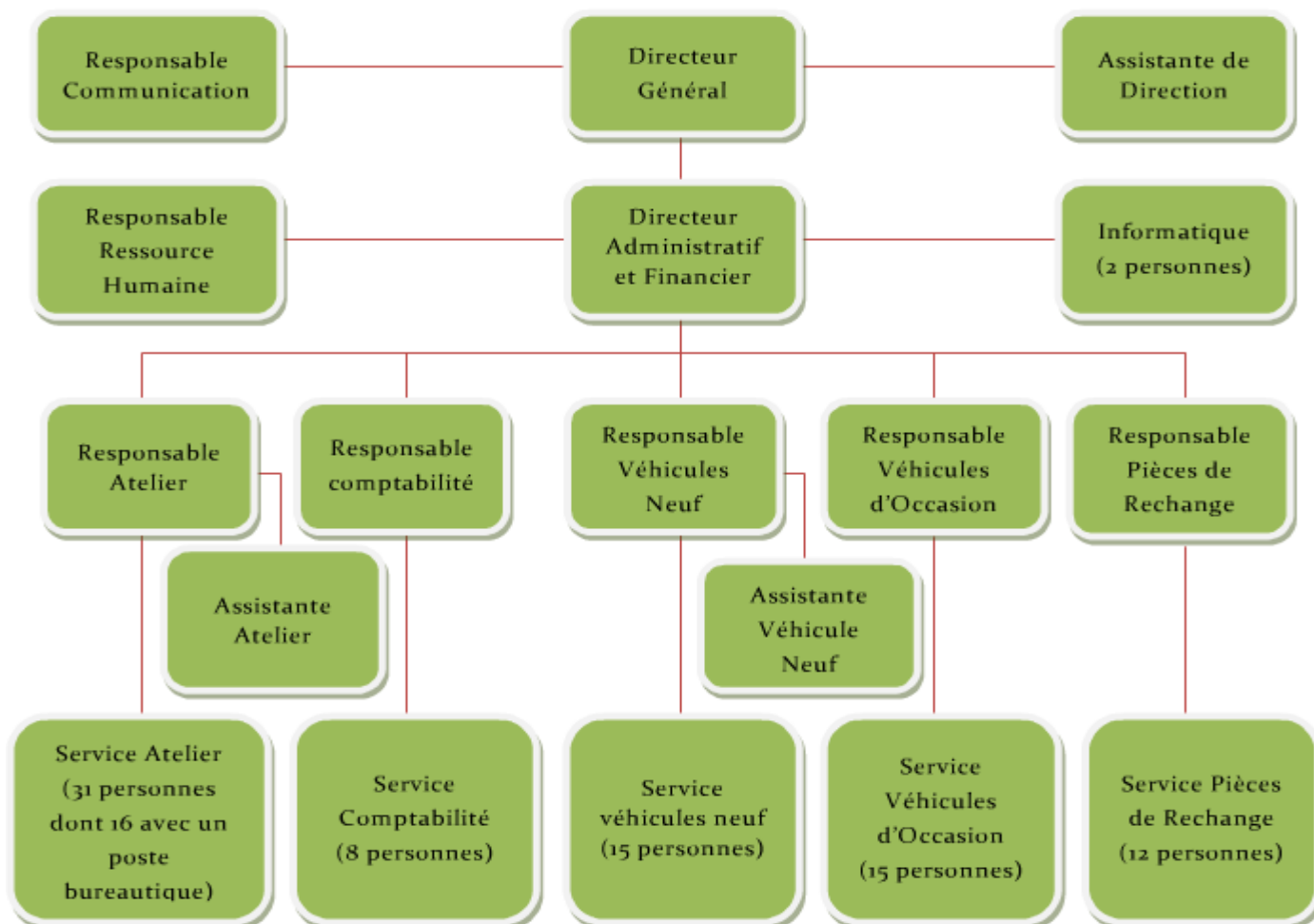
Mr PIGNER commença seul pour compter aujourd'hui 5 employés supplémentaires.

L'entreprise est une SARL.

L'entreprise peut compter sur la fidélité de ses clients et son savoir-faire dans l'industrie de l'informatique.

IV. Présentation du client

Notre client « **AutoConcept** » est un concessionnaire qui possède un parc informatique de 70 à 80 postes. La société est constituée de 83 employés répartis entre le service Atelier, le service Comptabilité, service Véhicule neuf, service Véhicule d'occasion, le service Pièce de rechange, le service informatique et la direction.



V. Note de synthèse

a. Introduction à la sécurité d'un système informatique

Parlons en premier des trois principaux termes liés aux risques pour la sécurité du système informatique d'une entreprise :

- La vulnérabilité représente le niveau d'exposition face à la menace
- Les menaces représentent le type d'action susceptible de nuire.
- Les contre-mesures sont l'ensemble des actions mises en œuvre en prévention de la menace.

On peut mettre cela sous la forme d'une équation :

$$\text{Risques} = (\text{Vulnérabilité} \times \text{Menaces}) / \text{Contre-mesures}$$

On voit donc que pour diminuer les risques, il faudrait diminuer la vulnérabilité du système et augmenter les contre-mesures. Ainsi, tout responsable de systèmes informatiques doit adopter des mesures de sécurité physiques (sécurité des systèmes d'information). Malheureusement, il n'est pas évident de mettre en place ces mesures sans atteindre aux libertés individuelles.

b. La sécurité des fichiers

Une politique de sécurité informatique est un plan d'actions définies pour maintenir un certain niveau de sécurité.

Voici les points autorisés et interdits pour mettre en place cette politique dans l'entreprise. Ainsi que les devoirs des responsables de sécurité.

- Tout traitement automatique est un plan d'actions définies pour maintenir un certain niveau de sécurité.
- Seules les personnes autorisées peuvent accéder aux données personnelles contenues dans un fichier. Il s'agit des destinataires explicitement désignés et des « tiers autorisés » ayant qualité pour les recevoir de façon ponctuelle et motivée (ex : la police, le fisc).
- Les administrateurs réseau et administrateur système sont tenus au secret professionnel et ne peuvent divulguer des informations même à leurs employeurs, sauf disposition législative particulière en ce sens.
- Il est autorisé de bloquer l'accès à certains sites web et l'utilisation de messageries instantanées, le téléchargement de logiciels, etc.

c. Informations à porter aux utilisateurs

Tout utilisateur est responsable de l'usage des ressources informatiques et du réseau auquel il a accès. Il a aussi la charge, à, son niveau, de contribuer à la sécurité générale des ressources de l'entité. L'utilisation de ces ressources doit être rationnel et loyal afin d'en éviter la saturation ou leur détournement à des fins autres que professionnelles.

Les utilisateurs des outils informatiques de l'entreprise doivent s'engager à :

- Ne pas accéder aux données d'un autre utilisateur sans l'autorisation de celui-ci.
- Ne pas modifier ou détruire des informations ne lui appartenant pas.
- Ne pas porter atteinte à l'intégrité ou à la sensibilité d'autres utilisateurs notamment par l'envoi de messages, textes ou images provocant.
- Ne pas développer ou utiliser des outils mettant sciemment en cause l'intégrité des systèmes d'informations.

L'utilisateur doit en particulier :

- Appliquer les recommandations de sécurité de l'entité à laquelle il appartient.
- Assurer la protection de ses informations, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels mis à sa disposition.
- Signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater.

- Suivre les règles en vigueur au sein de l'entreprise pour toute installation de logiciel.
- Choisir des mots de passes sûrs, gardés secrets et en aucun cas les communiquer à des tiers.
- Ne pas quitter son poste de travail ni ceux en libre-service sans se déconnecter en laissant des ressources ou services accessibles.

Il est donc nécessaire d'informer les utilisateurs du fonctionnement global du système et de la manière dont il peut et doit l'utiliser par l'intermédiaire d'une charte et de mémos internes afin d'éviter des problèmes juridiques en cas de conflits entre l'entreprise et le salarié.

d. Les dispositions légales pour le filtrage des contenus

Afin d'assurer une protection des intérêts légitime de l'entreprise et de limiter le risque de voir sa responsabilité engagée, l'employeur peut notamment mettre en place des dispositifs techniques interdisant l'accès à des sites non autorisés, interdire l'utilisation de messageries instantanées, le téléchargement de logiciels, etc. Concernant la messagerie électronique, il peut être mis en place des outils pour analyser les pièces jointes ou mesurer la fréquence ou la taille des messages.

VI. Sauvegarde et stockage des données sur le serveur

Les sauvegardes et le stockage des données seront enregistré dans un serveur présent dans nos locaux. La répartition de l'espace est :

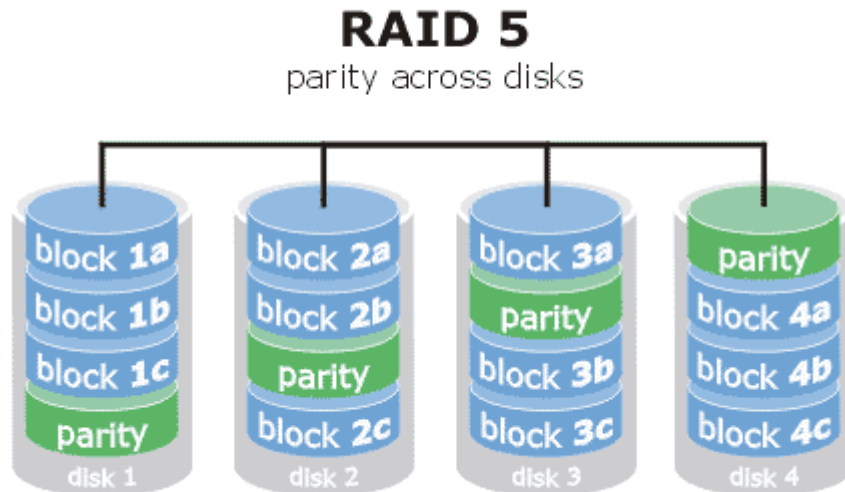
- 50Gb alloué à chaque post de l'entreprise.
- 2To d'espace supplémentaire à alloué sur demande à l'administrateur réseau.
- 2To d'espace de stockage spécial commun.

Cela représente donc 8To d'espace nécessaire pour le bon fonctionnement.

Le serveur sera un Fujitsu PRIMERGY HG-1. Il aura donc 2disques 4To (SOFT) ayant jusqu'à 4 places supplémentaire pour augmenter la capacité de stockage, les CPU sont 2 INTEL xeon E5-2640 v3 ayant 16coeurs, 32threads avec 128Go de mémoire RAM DDR4 ECC 2133MHz.

De plus nous ajouterons 2disques 4To à ce système.

Il ne restera plus que 2places supplémentaire mais la capacité de stockage sera doublée, et au niveau de la sécurisation des données nous auront 4disques ce qui nous permet de faire un raid 5.



VII. Mémo interne

L'informaticien doit porter la tenue qui lui a été fournie lors de son embauche par la société. Elle se compose obligatoirement d'un pantalon, polo ou t-shirt (au choix), d'une veste, d'un badge. Il doit également porter des chaussures de couleur noire.

Un vestiaire est mis à disposition et un cassier est attribué à chacun des employés pour leur tenue civile.

Une trace écrite de toute commande passer par les clients, des confirmations de livraisons, des garantis et des assurances devra être conservé par nous ainsi que par le client pour toute vérification à venir.

La communication entre collègues du service pour le bon fonctionnement de l'entreprise est obligatoire.

Tout logiciel installer devra avoir une License d'activation valide et officielle.

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

Tout rendez-vous pris pour une intervention doit être respecté ou le client doit être prévenu 48h avant intervention si celle-ci n'est plus possible aux horaires convenus.

Pour tout changement de matériel un accord préalable entre le technicien et le client ou son supérieur hiérarchique sera convenue et des interventions rapides seront effectuées.

Les clients seront tenus des avances des réparations effectuées sur leurs postes par les techniciens.

Les techniciens ne doivent en aucun cas consulter des fichiers ou dossier n'ayant aucun rapport avec les tâches à effectuer ou incident à résoudre sur les postes clients et en aucun cas les divulguer à un tiers.

Le respect des clients et un comportement professionnel est exigé de la part de chaque employé.

L'employé est responsable de l'entretien de ses tenues. Il doit se présenter sur son lieu de travail avec une tenue propre.

L'employé se doit de se présenter et d'informer les clients sur la nature et les actions qui seront faites lors de l'intervention.

L'employé se doit d'informer les clients sur les produits ainsi que les promotions et prendre en compte les demandes des clients pour appliquer les solutions adaptées.

VIII. Conclusion

Le but de ce projet était de proposer un système informatique sécurisé et fonctionnel pour la société AutoConcept à partir des éléments fournis par celle-ci.

Pour au final pouvoir externaliser la prestation informatique. Au cours de cette étude nous avons pu constater toutes les contraintes juridiques et les devoirs vis-à-vis des utilisateurs que nous avons pu clairement identifier.

Suite à cela nous avons été en mesure de fournir certaines solutions à cette société à travers divers documents.

Il fut possible de proposer de nouvelles règles pour améliorer leur sécurité ainsi qu'une charte de qualité pour rassurer le client. Il a été mis en place un mémo pour revoir considérablement les règles à suivre de la part de notre personnel au contact de nos clients.

Suite à vos pertes estimées à 140 000,00 € nous nous engageons sur la sécurisation des données qui est infaillible avec notre système.

Cette prestation est constituée de :

- d'une location d'un serveur physique (venant de nos locaux) avec un firewall et sa configuration.
- de frais de maintenance et préparation pour les 80 postes présents et le serveur physique.
- des licences officielles pour Windows 7 PRO, Office 2016 365 Business et Symantec anti-virus.

Le prix total de cette prestation est de : **29 178,89€ HT**

Nous espérons à présent que le client sera pleinement satisfait.

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

ANNEXE

I. Charte informatique

La charte informatique vous permet de définir les règles d'utilisation de l'Internet au sein de votre entreprise.

Ainsi, vous renforcerez la protection de votre réseau et, par-là même, vous pourrez veiller à ce que vos salariés n'abusent pas des outils mis à leur disposition.

L'entreprise MATI met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique.

Les salariés, dans l'exercice de leurs fonctions, sont conduits à accéder aux moyens de communication mis à leur disposition et à les utiliser.

L'utilisation du système d'information et de communication doit être effectuée exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte.

Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée du système d'information, la présente charte pose les règles relatives à l'utilisation de ces ressources.

D'une manière générale, l'utilisateur doit s'imposer le respect des lois et, notamment, celles relatives aux publications à caractère injurieux, raciste, pornographique, diffamatoire, sur le harcèlement sexuel/moral.

a) 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 (login + 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 la communiquer.

Un mot de passe doit, pour être efficace, comporter 12 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

b) Utiliser le 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 à la crypter.

Cette possibilité est offerte et disponible via le courrielleur (messagerie).

Il est interdit d'utiliser des services d'un site web spécialisé dans la messagerie.

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 365 jours et il existe des copies de sauvegarde pendant une période de 365 jours.

Ces copies de sauvegarde conservent tous les messages au moment où ils passent sur le serveur de messagerie, même s'ils ont été supprimés ensuite par leur destinataire.

c) 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.

d) Contrôle de l'usage

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

- le nombre des messages échangés de façon globale et par service.
- Le Directeur Général, son Assistante de Direction et le Responsable Communication le nombre des messages pouvant être échangés s'élève à 10 000.
- Le Directeur Administratif et Financier, le Responsable Ressources Humaine et la personne en charge de l'informatique le nombre des messages pouvant être échangés s'élève à 10 000.
- Le Responsable Atelier, son Assistante et le Service Atelier le nombre des messages pouvant être échangés s'élève à 5 000.
- Le Responsable Comptabilité et le Service Comptabilité le nombre des messages pouvant être échangés s'élèves à 10 000.

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

- Le Responsable Véhicule Neuf, son Assistance et le Service Véhicule Neuf le nombre des messages pouvant être échangés s'élèvent à 5 000.
- Le Responsable Véhicule Occasion et le Service Véhicule Occasion le nombre des messages pouvant être échangés s'élèvent à 5 000.
- Le Responsable Pièces de Rechange et le Service Pièces de Rechange le nombre de messages pouvant être échangés s'élèvent à 7 500.
- la taille des messages échangés.
- La taille des messages échangés correspond à la taille totale du mail (message, pièces jointes, signature). Elle est d'une taille maximale de 25Mo
- le format des pièces jointes.
- Les formats JPEG et PDF sont les seuls acceptés. La version PDF générée doit être à minima 1,5.

En cas d'un besoin spécifique s'adresser à l'Administrateur Réseau

e) 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 connecter un micro à Internet via un modem (*sauf autorisation spécifique*) ;
- de diffuser des informations sur l'entreprise via des sites Internet ;
- de participer à des forums (*même professionnels*) ;
- de participer à des conversations en ligne (« chat »).

f) 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.

g) Contrôles de l'usage

Dans l'hypothèse la plus courante, les contrôles portent sur :

- les durées des connexions

- les sites les plus visités

La politique et les modalités des contrôles font l'objet de discussions avec les représentants du personnel.

h) Configuration des postes utilisateur

La totalité des postes est mise à jour, les données sont récupérées et remises sur les postes ou serveurs sur des boîtes partagées selon la nature du fichier. L'installation de Windows 7 avec des licences officielles est effectuée, de même que le Pack Office 2016 365 Business (word, powerpoint, calc, excel, acces, one note, one drive, publisher) et le logiciel anti-virus est Symantec.

j) 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, l'échange de fichiers, et 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 (textes, images, vidéos ou logiciels) ;
- des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe (*et éventuellement texte du message*).

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, révisionniste ou contenant des données jugées comme offensantes.

Celui utiliser dans l'entreprise sera un Firewall ASA5520 qui sera configuré directement lors de la configuration serveur.

k) Sauvegardes

La mise en œuvre du système de sécurité comporte des dispositifs de sauvegarde des informations et un dispositif miroir destiné à sécuriser 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 en reste une copie :

- sur le serveur et son dispositif de sauvegarde

II. CHARTE QUALITE SERVICE CLIENT

La charte qualité de MATI traduit une valeur fondamentale de notre entreprise : l'amélioration continue de la satisfaction client dans l'ensemble des domaines d'intervention de notre société.

Pour permettre un traitement optimum et adapté des demandes de nos clients, nous avons défini une suite de procédures et d'action types permettant à notre équipe de définir et de répondre rapidement et de manière adaptée aux demandes des particuliers et des professionnels.

a) Nos engagements

Pour nos clients, tant particuliers que professionnels :

- Un délai d'intervention sous 24H
- Une réponse adaptée aux besoins du client
- Un suivi efficace de la relation client
- Une grille tarifaire explicite et visible
- Un strict respect des engagements contractuels
- La continuité de service en cas de panne

De plus, nous mettons à votre disposition à la personne ou à l'emplacement de votre choix les comptes rendus des interventions effectués, par ailleurs, nous pouvons établir des rendez-vous régulier avec l'un de nos Directeur Technique.

DEVIS SERVEUR

ABONNEMENT	Domaine	Quantité	Prix unitaire	Prix HT
Serveur Infrastructure HG - 128G 2xE5-2640v3 SoftRaid 2x4 To SAS - 12 mois	*001	1	4 199,88 €	4 199,88 €
Firewall ASA 5520 - 12 mois	*001	1	3 000,00 €	3 000,00 €
SOUS TOTAL				7 199,88 €

INSTALLATION	Domaine	Quantité	Prix unitaire	Prix HT
Frais d'installation du Firewall ASA 5520	*001	1	990,00 €	990,00 €
Préparation et mise à disposition de votre serveur	*001	1	0,00 €	0,00 €
Datacentre France	*001	1	0,00 €	0,00 €
SOUS TOTAL				990,00 €

 [Changer la durée de location](#) Durée choisie : 12 mois

ABONNEMENT	7 199,88 €
INSTALLATION	990,00 €

PRIX HT	8 189,88 €
TVA (20 %)	1 637,98 €
TOTAL TTC	9 827,86 €

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

DEVIS DE MAINTENANCE

ABONNEMENT	Domaine	Quantité	Prix unitaire	Prix HT
Maintenance des postes	*001	80	37,50€	3 000,00€
SOUS TOTAL				3 000,00€

INSTALLATION	Domaine	Quantité	Prix unitaire	Prix HT
Préparation et mise à disposition des postes	*001	80	25,00€	2 000,00€
Datacentre France	*001	1	0,00 €	0,00 €
SOUS TOTAL				2 000,00€

 [Changer la durée de location](#) Durée choisie : 12 mois

ABONNEMENT	3 000,00€
INSTALLATION	2 000,00€

PRIX HT	5 000,00€
TVA (20 %)	1 000,00€
TOTAL TTC	6 000,00€

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)
Tel : +33(0)5588770000
Email : contact@mati-informatique.com
<http://www.mati-informatique.com/>

DEVIS LOGICIELLE

ABONNEMENT	Domaine	Quantité	Prix unitaire	Prix HT
Licence Windows 7 Pro	*001	80	90,00€	7 200,00€
Licence Pack Office 2016 365 Business	*001		105,60€	8 448,00€
Anti-virus Symantec	*001		19,46€	1 556,80€
SOUS TOTAL				17 204,80€

 [Changer la durée de location](#) Durée choisie : 12 mois

ABONNEMENT	17 204,80€
------------	------------

PRIX HT	17 204,80€
TVA (20 %)	3 440,96€
TOTAL TTC	20 645,76€

MATI – 18 avenue de la Paix – 92 000 NANTERRE (France)

Tel : +33(0)5588770000

Email : contact@mati-informatique.com

<http://www.mati-informatique.com/>

III. Textes de Lois

Les lois énoncées dans ce document sont données à titre purement indicatif, à la date d'édition du présent document et de manière non exhaustive.

a) Délit informatiques

La loi française reconnaît certaines actions sur les systèmes informatiques comme étant des délits et prévoit de les sanctionner.

À titre d'exemple :

-La loi dite « Godfrain » du 5 Janvier 1988 (n° 88-19) a introduit dans le code pénal l'article 462-2 a créé le délit d'intrusion dans un système informatique.

-La loi « pour la confiance dans l'économie numérique » du 21 juin 2004 (n° 2004-575) a déplacé et modifié ce texte, désormais présent à l'article 323-1 du code pénal, lequel dispose que *« 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. »*

b) Sanctions pénales

L'Entreprise est tenue par la loi de signaler toute violation constatée des lois. Les sanctions pénales peuvent aller de 1 mois à plusieurs années de prison et de 300 euros à plusieurs centaines de milliers d'euros d'amende. Les principales lois françaises et européennes sont :

- le code de propriété intellectuelle
- la loi du 06/01/1978 sur l'informatique, la sécurité et les libertés
- La loi du 03/07/1985 sur la protection des logiciels,
- les articles 462.2 à 462-9 du code pénal
- la convention européenne du 28/01/1981 pour la protection des personnes à l'égard du traitement informatisé des données à caractère personnel
- la directive de la CEE du 21/12/1988 sur l'harmonisation juridique de la protection des logiciels.

Extraits du code de propriété intellectuelle

Art.L335-2 Entrée en vigueur 2016-06-05

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende.

Seront punis des mêmes peines le débit, l'exportation, l'importation, le transbordement ou la détention aux fins précitées des ouvrages contrefaisants.

Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende.

Art.L335-3

Est également un délit de contrefaçon toute reproduction, représentation ou diffusion, par quelque moyen que ce soit, d'une œuvre de l'esprit en violation des droits de l'auteur, tels qu'ils sont définis et réglementés par la loi.

Est également un délit de contrefaçon la violation de l'un des droits de l'auteur d'un logiciel définis à l'article [L. 122-6](#).

Article 462-2

Quiconque, frauduleusement, aura accédé ou se sera maintenu dans tout ou partie d'un système de traitement automatisé de données sera puni d'un emprisonnement de deux mois à un an et d'une amende de 2 000 F à 50 000 F ou de l'une de ces deux peines. Lorsqu'il en sera résulté soit la suppression ou la modification de données contenues dans les systèmes, soit une altération du fonctionnement de ce système, l'emprisonnement sera de 2 mois à 2 ans et l'amende de 10 000 F à 100 000 F.

Article 462-3

Quiconque aura, intentionnellement et au mépris des droits d'autrui, entravé ou faussé le fonctionnement d'un système de traitement automatisé de données sera puni d'un emprisonnement de trois mois à 3 ans et d'une amende de 10 000 F à 100 000 F ou de l'un de ces deux peines.

Article 462-4

Quiconque aura, intentionnellement et au mépris des droits d'autrui, directement ou indirectement, introduit des données dans un système de traitement automatisé ou supprimé ou modifié les données qu'il contient ou leurs modes de traitement ou de transmission sera puni d'un emprisonnement de 3 mois à 3 ans et d'une amende de 2000 F à 500 000 F ou de l'une de ces deux peines.

Article 462-5

Quiconque aura procédé à la falsification de documents informatisés, quelle que soit leur forme, de nature à causer un préjudice à autrui, sera puni d'un emprisonnement d'un an à cinq ans et d'une amende de 20 000 F à 2 000 000 F.

Article 462-6

Quiconque aura sciemment fait usage des documents visés par l'article 462-5 sera puni d'un emprisonnement d'un an à cinq ans et d'une amende 20 000 F à 2 000 000 F ou de l'une de ces deux peines.

Article 462-7

La tentative des délits prévus par les articles 462-2 à 462-6 est punie des mêmes peines que le délit lui-même.

Article 462-8

Quiconque aura participé à une association formée ou à une entente établie en vue de la préparation, concrétisée par un ou plusieurs faits matériels, d'une ou plusieurs infractions prévues par les articles 462-2 à 462-6 sera puni des peines prévues pour l'infraction elle-même ou pour l'infraction la plus sévèrement réprimée.

Article 462-9

Le tribunal pourra prononcer la confiscation des matériels appartenant au condamné et ayant servi à commettre les infractions prévues au présent chapitre.