

Étude de Cas GMSI Région 2020

Projet SAS



Alexandre LASSUYT, Matthieu LINARD, Gérard MOLINA, Bénédicte NICOLATS

Table des matières

1	Présentation de la société JASSUR Informatique	5
2	Présentation de la société « AutoConcept » et de son projet	6
3	Le cahier des charges qui en découle.....	7
4	Note de Synthèse sur les problématiques, notamment du point de vue légal, d'utilisation des outils informatiques en entreprise.....	9
4.1	Cadre légal d'utilisation des moyens informatiques :.....	9
4.2	Les moyens mis en œuvre pour la sécurité des fichiers	11
4.3	Les informations à transmettre aux employés concernant l'utilisation des outils informatiques	13
4.4	La solution de filtrage.	15
5	Établissement d'un plan de sécurisation.....	18
5.1	Politique de sécurité des mots de passe.....	18
5.2	Les mesures immédiates de sauvegarde	19
6	La charte « Qualité Service client »	20
6.1	De façon générale	20
6.2	La continuité de service en cas de panne.	21
6.3	Le relationnel client.	21
7	Sécurité et productivité garantie par JASSUR Informatique	22
8	Proposition de mémo sur la conduite à tenir chez un client.	23
9	Conclusion	24
10	Annexe 1 : Organigramme de JASSUR Informatique.....	25
11	Annexe 2 : Charte graphique de JASSUR Informatique.....	26
12	Annexe 3 : Organigramme « AutoConcept »	27
13	Annexe 4 : Compte rendu du service commercial de « AutoConcept »	28
14	Annexe 5 : Textes de loi.....	29
15	Annexe 6 : Enquête de satisfaction	33
16	Annexe 7 : Fiche d'intervention JASSUR Informatique	34
17	Annexe 8 : Proposition de Contrat SLA	35
18	Annexe 9 : Plan de Veille	36
19	Annexe 10 : Gestion de projet.....	37
20	Notre ressenti.....	38
21	Glossaire	39
22	Bibliographie	40

1 Présentation de la société JASSUR Informatique

Elle fut créée en 2015 par Alexandre LASSUYT, Gérard MOLINA, Bénédicte NICOLATS

Au démarrage, une petite équipe dynamique et qualifiée qui a su s'adapter rapidement à la demande croissante en étoffant son personnel. Nous sommes actuellement au nombre de sept et nous sommes en recherche de techniciens. Organigramme : voir [Annexe 1](#)
Charte graphique [Annexe 2](#)

[Adresse](#) : 7 bis Avenue Robert Schuman, 51100 Reims

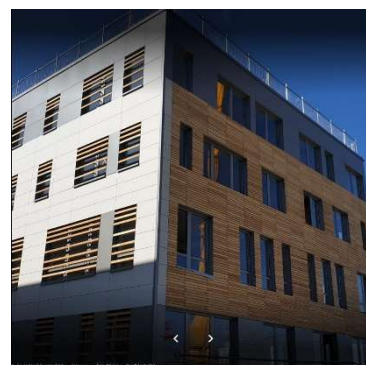
[Horaires](#) : Lundi au Vendredi 09H00-18H00
Samedi 08h00-13h00

[Téléphone](#) :
03 LA LM MG NB

[Téléphone SAV](#) : Du lundi au samedi 19h00
06 LA LM MG NB

[Mail](#) : contact@jassurinformatique.fr

[Site Web](#) : jassur-informatique.fr



Notre accompagnement dans :

- L'analyse de la situation de l'entreprise
- L'élaboration de votre projet de parc informatique
- La réalisation de son installation
- La maintenance
- Son maintien à niveau

Chaque projet est unique, nous nous adaptons aux besoins de votre entreprise, nous sommes à vos côtés dans votre quotidien. Nos experts sont à votre écoute pour vous aider à optimiser votre matériel afin que votre parc informatique ne soit plus un frein à votre développement mais un outil primordial.

Nous nous sommes spécialisés dans les PME et les TPE.
Nous travaillons dans l'Aisne, les Ardennes et la Marne.

Ils nous font confiance :



2 Présentation de la société « AutoConcept » et de son projet

Suite à l'audit réalisé par notre société à votre demande, nous avons relevé de gros problèmes de sécurisation de ce système et une organisation du service informatique qui pourrait être améliorée.

Comme documents de travail, nous avons :

Votre organigramme de société [Annexe 3](#)

Le compte rendu de votre service commercial [Annexe 4](#)

Résultats de notre audit

Au niveau hardware :

- Des ordinateurs trop lents en fonctionnement
- Une sauvegarde des données insuffisante

Au niveau de l'utilisation du parc :

- Sécurité insuffisante au niveau des utilisateurs, pas d'identification, ni de mot de passe.
- Un logiciel d'exploitation non officiel
- Pas de sécurisation de vos données
- Pas de charte d'utilisation du matériel informatique

Votre service informatique :

- Intervention manquant de rapidité
- Manque de professionnalisme
- Pas de respect de la confidentialité
- Une communication non adaptée
- Non-respect des délais
- Utilisateur ne connaissant pas les logiciels ou application non autorisés
- Changement de matériel non demandé

3 Le cahier des charges qui en découle

Réaliser une note de synthèse sur les problématiques (du point de vue de la loi) d'utilisation des outils informatiques en entreprise. Il veut savoir ce que la loi l'autorise à mettre en œuvre, et ce que les utilisateurs peuvent faire.

Il souhaiterait que vous portiez une attention particulière sur les points suivants :

- Quelles sont les règles régissant l'utilisation des moyens informatiques mis à disposition des salariés,
- Quels moyens doivent être mis en œuvre pour la sécurité des fichiers,
- Quelles informations doivent être portées aux personnes dans l'entreprise concernant l'utilisation des outils informatiques,
- Quelles sont les dispositions légales concernant la mise en place d'une solution de filtrage de contenus en entreprise.

Établir un plan de sécurisation des données

- Politique de sécurité de mot de passe, modalités de communication aux utilisateurs et de mise en œuvre
- Mesures immédiates de sauvegarde.

Rédiger des propositions sur les engagements qualité qui seront consignés dans une charte « Qualité Service Client » remise avec la proposition au client. La consigne est de rassurer le client et marquer une différence notable en qualité de service par rapport à l'existant.

Il est impératif de faire la différence sur :

- La continuité de service en cas de panne
- Le relationnel client
- La sécurité et la productivité

Rédiger une proposition de mémo qui sera diffusé en interne chez JASSUR Informatique (notamment aux nouveaux) sur la conduite à tenir chez un client. Il vous conseille de vous appuyer sur les plaintes-clients remontées par le service commercial.

L'utilisation de l'informatique en entreprise

De nos jours, il n'est plus possible de ne pas avoir de matériel informatique dans sa société. Que ce soit par l'utilisation d'ordinateurs, de smartphones, de tablettes, d'imprimantes, de fax, l'informatique est au cœur de nos vies.

S'il est plus ou moins facile de l'installer, d'apprendre à s'en servir, il se révèle plus compliqué d'en avoir une utilisation optimale et sécurisée.

Toute mauvaise utilisation peut avoir des conséquences néfastes pour l'entreprise, la connexion internet est une porte ouverte à toute attaque cybernétique.

La perte d'information peut avoir un coût financier important.

La mauvaise gestion du parc informatique ainsi qu'une mauvaise image du service informatique peut être préjudiciable à la société.

Quelles sont les obligations des entreprises, et celles des employés ?

Dans un premier temps, nous allons voir les devoirs et obligations liés à l'utilisation de l'informatique par le biais de la législation en vigueur, des moyens existants pour la sécurité des fichiers, les informations d'utilisation données aux employés ainsi qu'une solution de filtrage que peut proposer une société.

Dans un second temps, nous parlerons du plan de sécurisation des données.

Nous continuerons par des suggestions pour la chartre qualité de JASSUR Informatique donnée à chaque entreprise.

Nous terminerons par le Mémo de JASSUR Informatique qu'il fait signer à chacun de ses employés.

4 Note de Synthèse sur les problématiques, notamment du point de vue légal, d'utilisation des outils informatiques en entreprise

4.1 Cadre légal d'utilisation des moyens informatiques :

Les outils informatiques ainsi que l'informatisation ont permis de simplifier la vie des entreprises.

Travail plus rapide, un gain de temps donc une meilleure productivité ; des fichiers accessibles rapidement par tous sans déplacement, mutualisation des ressources, ...

Que va-t-il arriver s'il y a un problème lié à l'utilisation de ces outils ?

C'est pour définir les devoirs et obligations de chacun que différentes lois ont été créées.

Les textes de loi ou les textes des différents codes sont regroupés dans l'[Annexe 5](#).

La toute première loi est la Loi Informatique et Libertés, créée en 1978 et modifiée en 2004, concerne l'ensemble des traitements informatisés de données personnelles.

Il y a création de la CNIL.

Elle est chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques ou papiers, aussi bien publics que privés.

Elle a un rôle d'alerte, de conseil et d'information pour tous les publics mais a aussi un pouvoir de contrôle, de sanction et d'anticipation.

Son cadre :

- L'obligation de déclarer auprès de la CNIL les fichiers contenant des données personnelles
- L'interdiction de collecter des données à caractère sensible, c'est-à-dire relatives à la religion, la santé, la politique, ...
- Le principe de collecte loyale de données
- L'obligation d'assurer la sécurité de l'ensemble des données collectées
- L'obligation d'informer les individus concernés de la collecte de leurs données
- Le droit à l'accès, la modification et la suppression des données en question

La loi 2018-493 du 20 juin 2018 voit la mise en place concrète du RGPD qui accompagne la CNIL.

Il permet :

- Une uniformisation européenne
- Un renforcement du droit des personnes quant à l'utilisation de leurs données personnelles
- Simplifier l'environnement réglementaire des entreprises

Il préconise :

- Instaurer un correspondant informatique et libertés qui doit informer, conseiller et contrôler
- Faire des registres de traitement des données personnelles et trier les données
- Afin de suivre la réglementation actuelle et à venir, définir les axes d'action en fonction des risques liés à aux recueils des données personnelles
- S'il existe des risques élevés il faut faire une analyse d'impact relative à la protection des données
- Pour maintenir un niveau élevé de protection des données personnelles, il faut instaurer des procédures internes et faire de la veille
- Toutes les actions doivent être mises par écrit et doivent être réactualiser régulièrement.

Ces deux lois concernent le recueil des données personnelles mais il en existe d'autres qui s'appliquent aussi pour « AutoConcept »

L'utilisation de logiciels doit se faire dans le respect de la propriété intellectuelle et des recommandations fixées par les détenteurs de droit et des engagements pris par l'entreprise

Loi 92-597 du 1 juillet 1992

Les textes législatifs ne sont pas les seuls à définir de cadre législatif. Il existe aussi des directives imposées par le **code du travail** :

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché » Article L1121-1

Obligation d'informer le comité d'entreprise avant la mise en place de nouvelles technologies
Article 432-2.

Une question revient régulièrement dans les entreprises.
L'employé peut-il utiliser à titre privé les outils informatiques de la société ?

Là s'applique le bon sens, si le travail du salarié n'est pas affecté et que la sécurité des réseaux n'est pas mise en danger, l'employeur peut tolérer cette utilisation dans la mesure du raisonnable.

Le contrôle de l'utilisation d'internet et de la messagerie électronique est un sujet essentiel régulé par la Commission Nationale Informatique et Libertés (CNIL). « *L'utilisation, sur les lieux de travail, de ces outils informatiques à des fins autres que professionnelles est généralement tolérée. Elle doit rester raisonnable et ne doit pas affecter la sécurité des réseaux ou la productivité de l'entreprise ou de l'administration concernée* ».

S'il y a litige, faute ou non application de la loi,
Il est possible pour l'employé et/ou l'employeur de saisir :

- L'inspection du Travail,
- Le procureur de la République,
- Le service des plaintes de la CNIL

Ces différents éléments définissent le cadre juridique de l'utilisation des outils informatiques.

Il est connu que très souvent les problèmes liés à l'informatique sont plutôt liés à une mauvaise utilisation de cette dernière volontairement ou non. Il revient donc à l'entreprise de mettre en place des moyens de limitations d'erreur, afin d'aboutir à une meilleure sécurité informatique.

4.2 Les moyens mis en œuvre pour la sécurité des fichiers

Concevoir une procédure de création et de suppression des comptes utilisateurs

L'accès aux postes de travail et aux applications doit s'effectuer à l'aide de comptes utilisateurs nominatifs (prénom+nom), et non « génériques » (compta1, compta2...), ainsi la direction, l'administrateur pourra si besoin tracer les actions faites sur un fichier. Ce qui permet ainsi de responsabiliser l'ensemble des intervenants. Cette règle doit aussi s'appliquer aux comptes des administrateurs systèmes et réseaux et des autres agents impliqués.

Identifier précisément qui peut avoir accès aux fichiers

L'accès aux données personnelles traitées dans un fichier doit être limité aux personnes qui en ont besoin pour leurs missions. Ainsi le responsable hiérarchique définit « le profil d'habilitation » de l'agent ou du salarié concerné. Il faut procéder ainsi pour chaque évolution ou nouvelle affectation d'un salarié.

Une vérification périodique des profils des applications et des droits d'accès est nécessaire afin de s'assurer de leur bon fonctionnement.

Sécuriser les postes de travail

Sécuriser les connexions implique un verrouillage automatique au-delà d'une période d'inactivité (10 minutes maximum). Les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Il est aussi fortement recommandé de contrôler l'usage des ports USB sur les postes « sensibles », bloquant par exemple la copie de l'ensemble des données contenues dans un fichier.

Veiller à la confidentialité des données vis-à-vis des prestataires

Les interventions des sous-traitants du système d'information doivent présenter les garanties suffisantes (sécurité et confidentialité) vis-à-vis des données auxquelles ils peuvent avoir accès. La loi impose ainsi une clause de confidentialité dans les contrats de sous-traitance. Toute intervention d'un prestataire sur des bases de données doit se dérouler en présence d'un salarié du service informatique et être consignée. Les données considérées « sensibles » au regard de la loi, par exemple des données de santé ou des données relatives à des moyens de paiement, doivent en plus faire l'objet d'un chiffrement.

« A noter » : l'administrateur systèmes et réseaux n'est pas forcément habilité à accéder à l'ensemble des données de l'organisme. Les données peuvent être chiffrées avec une clé dont il n'a pas connaissance, ainsi il peut réaliser ses missions sans accéder aux données en clair.

Sécuriser le réseau local

Un système d'information doit être sécurisé vis-à-vis des attaques extérieures. Un premier niveau de protection doit être assuré par des dispositifs de sécurité logique spécifiques tels que des routeurs filtrants (ACL), pare-feu, sondes anti-intrusions, etc.

Il est aussi indispensable de sécuriser les réseaux sans fil compte tenu de la possibilité d'intercepter à distance les informations qui y circulent : utilisation de clés de chiffrement, contrôle des adresses physiques des postes clients autorisés, etc.

Une veille constante est nécessaire pour maintenir et mettre à jour les différents éléments de sécurité. La messagerie électronique doit aussi faire l'objet d'une vigilance particulière.

Enfin, les accès distants au système d'information par les postes nomades (déplacements, télétravail, etc.) doivent être prévus et sécurisés. Les accès par internet aux outils d'administration électronique nécessitent également des mesures de sécurité fortes (utilisation de protocoles IPsec, SSL/TLS ou encore HTTPS).

Sécuriser l'accès physique aux locaux

L'accès aux locaux sensibles, tels que les salles hébergeant les serveurs informatiques et les éléments du réseau, doit être limité aux personnels habilités. Ces locaux doivent faire l'objet d'une sécurisation particulière (vérification des habilitations, gardiennage, portes fermées à clé, digicode, contrôle d'accès par badge nominatifs, etc.)

La DSI ou le responsable informatique doit veiller à ce que les documentations techniques, plans d'adressages réseau, contrats, etc. soient eux aussi protégés.

Anticiper le risque de perte ou de divulgation des données

La perte ou la divulgation de données peut avoir plusieurs origines : erreur ou malveillance d'un salarié ou d'un agent, vol d'un ordinateur portable, panne matérielle, ou encore conséquence d'un dégât des eaux ou d'un incendie. Pour limiter ce risque il faut veiller à stocker les données sur des espaces serveurs prévus à cet effet et avec des sauvegardes régulières.

Les supports de sauvegarde doivent être stockés dans un local distinct de celui qui héberge les serveurs (idéalement dans un coffre ignifugé). Les serveurs hébergeant des données sensibles ou capitales pour AutoConcept doivent être sauvegardés et pourront être dotés d'un dispositif de tolérance de panne. Il est recommandé d'écrire une procédure « urgence – secours » qui décrira comment remonter rapidement ces serveurs en cas de panne ou sinistre majeur.

Les supports nomades (ordinateurs portables, clé USB, etc.) doivent faire l'objet d'une sécurisation particulière, par chiffrement, vu la sensibilité des dossiers ou documents qu'ils peuvent stocker. En outre, les matériels informatiques en fin de vie, tels que les ordinateurs ou les copieurs, doivent être physiquement détruits avant d'être jetés, ou a minima expurgés de leurs disques durs avant de s'en séparer.

Anticiper et formaliser une politique de sécurité du système d'information

L'ensemble des règles relatives à la sécurité informatique doit être formalisé dans un document présenté à l'ensemble du personnel. Sa rédaction nécessite de faire d'abord l'inventaire des menaces et vulnérabilités qui pèsent sur un système d'information.

Il est indispensable de faire évoluer régulièrement ce document, en fonction des modifications des systèmes et outils informatiques utilisés par AutoConcept. Enfin, le paramètre « sécurité » doit être pris en compte en amont de tout projet lié au système d'information.

Les informations transmises aux employés.

4.3 Les informations à transmettre aux employés concernant l'utilisation des outils informatiques

Les risques encourus par l'entreprise à cause d'un manque de sécurité informatique sont divers.

Parmi eux, il peut être citer :

- Les rançongiciels : des programmes malveillants qui chiffrent les données personnelles de l'entreprise dans le but de lui extorquer de l'argent,
- Le piratage des données relatives à l'activité et au savoir-faire de la structure,
- La divulgation de fausses informations sur les réseaux,
- Le piratage de compte.

Pour se protéger contre ces menaces, il est nécessaire de communiquer au personnel de l'entreprise des mesures à respecter.

Le mot de passe

Étant un moyen d'authentification pour accéder à ses équipements ou ses données, il est donc important de bien le choisir. De plus, il est personnel et ne doit rester à la portée de personne. A noter aussi que le service informatique ne vous demandera jamais de communiquer votre mot de passe par mail, formulaire ou par téléphone.

Pour le composer, utilisez entre 8 et 12 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux) n'ayant aucun lien avec vos noms et date de naissance. Il doit également être unique pour chaque application. Vous pouvez, par exemple, utiliser une logique de déplacement sur le clavier pour se faire. Par exemple : `w!x:c;123MLK` (analysez le positionnement de ses caractères sur le clavier, pour vous faire une idée).

Veillez également à le changer toutes les deux semaines en vous référant au mode de composition renseigné ci-dessus.

Mise à jour régulière des logiciels

Respectez la politique de mise à jour des logiciels de manière régulière afin de limiter au maximum la vulnérabilité des systèmes d'exploitation et risquer au minimum l'espionnage de votre activité.

La fiabilité des liens internet

En effet, courriels, pièces jointes et liens internet peuvent être porteur de virus : assurez-vous de leur provenance avant de lancer leur ouverture. Aussi par sécurité, n'utilisez pas votre ordinateur professionnel dans le cadre d'une utilisation privée.

Communication intranet

N'utilisez que les modes de communication mis en place par la structure :

- Microsoft Outlook (compte professionnel) ;
- Messagerie SISCO
- Teams

Ne pas utiliser de surface de stockage externe à l'entreprise

Vos téléphones portables ainsi qu'une clé USB peuvent être source de virus et de logiciels malveillants. Veillez à ne jamais les connecter à un ordinateur de la société ou à un périphérique réseau.

Précautions lors des déplacements

- Marquez votre équipement afin d'éviter les confusions de matériel,
- Utilisez un filtre pour votre écran,
- N'utilisez que votre équipement professionnel,
- Sauvegardez régulièrement vos données pour éviter les pertes,
- Ne pas préenregistrer les mots de passe,
- Gardez vos équipements en votre possession tout au long du déplacement,
- Désactivez le Wifi et le Bluetooth pendant les trajets,
- Si vous êtes contraints de vous séparer de vos équipements, retirez les batteries

Pour toutes questions ou informations, renseignez-vous auprès de votre référent numérique soit directement soit par téléphone : Monsieur SOULET au 06 33 16 64 51.

Des moyens de sécuriser les données de la société sont instaurés, l'employé connaît ses droits et ses obligations quant à l'utilisation du matériel et des logiciels mis à sa disposition. Il est conseillé d'aller plus loin dans la sécurisation des informations ainsi que dans la qualité d'utilisation de l'informatique. La société doit protéger l'utilisation interne de son réseau et se prémunir d'éventuelles intrusions externes.

4.4 La solution de filtrage.

La société a aussi des obligations de moyens pour protéger son réseau

- Contre la consultation de sites racistes, négationnistes,
- Contre l'achat de produits dont la vente est interdite sur Internet (certains médicaments, alcool, tabac).
- Elle a aussi des obligations de sécurisation de son réseau contre le piratage
- Des obligations de conserver les logs (données de connexion) pendant un an
- Des obligations de la mise en place d'une charte informatique
- Des obligations de déclaration à la CNIL si mise en place de collecte d'informations nominatives

L'entreprise pourra donc, de façon à prouver un abus, utiliser plusieurs choses :

- Les données relatives au trafic
- Les données d'identifications
- Les données de connexion.

La direction de « AutoConcept » peut répondre à tous ces points en mettant en place une solution de filtrage des contenus en entreprise. Car elle est responsable civilement et / ou pénalement de l'utilisation en interne de son système informatique, quels que soient les utilisateurs.

Qu'est-ce que le filtrage ?

Solution légale permettant de protéger des utilisations frauduleuses des données et des intrusions malveillantes dans les systèmes informatiques. Sa non-application engage la responsabilité de l'entreprise pour toute utilisation illégale.

La décision 276/1999 CE du 25 janvier 1999 du Parlement européen et du Conseil adoptant un plan visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. Les outils de filtrage constituent des éléments essentiels pour assurer un environnement plus sûr sur Internet.

La loi antiterroriste du 23 janvier 2006 étend aussi à l'entreprise entre autres l'obligation de mettre en place des filtres et de conserver pendant un an les données de connexion, imposée aux fournisseurs d'accès Internet (FAI) par l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN).

Avant toute chose, l'employeur est obligé de prévenir son personnel qu'un moyen de filtrage et donc de récupération des données est mis en place. Article L121-8 du code du travail. Article L122-4

La CNIL préconise alors une consultation du comité d'entreprise (guide pratique de la CNIL pour les employeurs et les salariés) ainsi qu'une déclaration auprès de cette dernière (La Cyber surveillance sur les lieux de travail de la CNIL).

Dès qu'il y a recueil de données, l'employeur doit tout faire pour la sécurité de ces dernières et informer les utilisateurs des risques encourus. Directive européenne 2002-58 du 12 juillet 2002. L'employeur est responsable des données recueillies et doit veiller à une bonne utilisation. Loi 92-684 du 22 juillet 1992.

La mise en place du filtrage ne peut être restrictive quant aux limitations des droits des personnes. Article L1121-1 du code du travail.

L'employeur peut utiliser les logs de connexion afin de connaître l'historique de ses employés sur internet mais uniquement ceux à caractère professionnel. Dans l'arrêt du 9 juillet 2008, la cour de Cassation stipule que l'employeur peut rechercher ces données même hors de la présence de l'employé.

Les recommandations du Comité des ministres aux États membres :

- La recommandation 2008-6 sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet
- La recommandation 2001-8 sur l'autorégulation des cyber-contenus,
- La recommandation 2007-11 sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication.

Quand est-il de la responsabilité de tout salarié ?

Extrait du code civil :

« Tout fait quelconque de l'homme, qui cause à autrui un dommage, oblige celui par la faute duquel il est arrivé à le réparer »

« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence »

Ces extraits stipulent clairement que le salarié est responsable de ses actes, même involontaires. La session utilisateur est personnelle et ne doit en aucun cas être utilisée par quelqu'un d'autre. Tout acte défendu, ou illicite peut entraîner des poursuites et/ou obliger le propriétaire du compte utilisateur à réparer ses torts.

Les administrateurs peuvent aussi avoir un rôle ?

Ils sont au même titre que chaque employé responsable de leurs actes.

Ils doivent informer la direction des moyens de filtrage qui existent et les maintenir à jour.

Ils sont les garants de la bonne pratique du filtrage.

L'employeur a pour obligation de prévenir ses salariés sur les bonnes pratiques de l'utilisation des outils informatiques mis à leur disposition ainsi que la mise en place d'un système de filtrage. Cela permet de faire un pas supplémentaire dans la sécurisation du système informatique.

A ce stade, il est vivement conseillé d'instaurer une charte d'utilisation informatique qui sera signée par tous les salariés et mis en annexe du règlement intérieur. Cette charte peut être réalisée en collaboration avec JASSUR Informatique ainsi qu'avec l'inspection du travail pour le côté purement juridique.

Dans les demandes « d'AutoConcept », il y avait aussi un gros problème sur la sécurisation des données : intrusion d'un client sur un poste d'une commerciale, perte de données après un crash.

Il va falloir porter une attention particulière à une politique de sécurisation des mots de passe ainsi qu'à des mesures de sauvegarde.

5 Établissement d'un plan de sécurisation

De nos jours, il est demandé constamment d'inscrire un mot de passe pour accéder à tout matériel informatique : smartphone, tablette, ordinateur, logiciel, ...
Comment les générer, les instaurer, ...

5.1 Politique de sécurité des mots de passe

Inspiré de SSI. Gouv, guide des bonnes pratiques de l'informatique
Ainsi que de la CNIL authentification par mot de passe, les mesures élémentaires

La refonte de l'organisation des mots de passe devra être planifiée à l'avance et testée avant d'être déployée à la date prévue, en accord avec l'entreprise.

La 1^{re} élaboration de mots de passe pour tous les salariés est à effectuer par le staff technique, chaque mot de passe est à accès strictement personnel et ne permet d'accéder qu'aux contenus nécessaires aux fonctions de chaque salarié. Le système doit obliger l'utilisateur à changer de mot de passe lors de la 1^{re} connexion.

Les accès seront bien sûr limités aux fonctions de chaque salarié, après discussion avec les différents responsables, à l'aide de comptes nominatifs.

La communication des mots de passe doit se faire en propre (papier)

Le staff technique devra configurer l'obligation de changer de mot de passe tous les 3 mois, responsabilité à la charge des employés. Un guide pour bien choisir son mot de passe leur sera fourni.

Notamment 2 méthodes simples :

- La méthode phonétique : « J'ai acheté 5 CDs pour cent euros cet après-midi » : ght5CDs%E7am ;
- La méthode des premières lettres : « Allons enfants de la patrie, le jour de gloire est arrivé » : aE2IP,IJ2Gea!

Personne ne leur demandera jamais leur mot de passe, staff technique ou autre. Il faudra s'assurer que tout le monde retienne les règles de sécurité. Ne jamais le transmettre ni l'utiliser en dehors des moyens sécurisés énoncés par la charte de sécurité.

Les postes des agents doivent être paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité (10 minutes maximum) ; les utilisateurs doivent également être incités à verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau.

En cas d'oubli de mot de passe, le responsable de traitement appliquera une procédure de renouvellement du mot de passe (remis en mains propres)

5.2 Les mesures immédiates de sauvegarde

Tout réseau informatique est exposé à des risques issus d'une mauvaise intention comme le détournement de données ou d'un problème technique comme une panne ou une surchauffe. Afin de les éviter, il est nécessaire de mettre en place un plan de sécurisation du parc informatique.

Le protocole peut se scinder en quatre points :

Sécuriser et minimiser les accès aux serveurs en les disposant dans une salle climatisée afin d'éviter les risques de surchauffe et donc de pertes de données potentielles. Dans un second temps, les positionner le plus au centre du bâtiment afin de réduire les possibilités d'accès de l'extérieur au maximum. Verrouiller l'accès aux personnes étrangères au support informatique et sécuriser le local au moyen d'une porte coupe-feu à verrou codée. Il est aussi possible de stocker les données auprès d'un hébergeur reconnu tel que Amazon.

Concernant la gestion des accès informatiques, il est nécessaire de créer au sein de l'entreprise des profils utilisateurs afin que chaque employé de la société AutoConcept ne puisse avoir accès qu'aux données et applications dont il a besoin dans le cadre de ses fonctions. Il est également préférable de limiter les droits d'actions tels que la suppression de données. Il serait vivement recommandé de protéger les postes informatiques à l'aide d'un identifiant et d'un mot de passe connu uniquement par leur utilisateur, le dirigeant et le support informatique.

La gestion des systèmes de sauvegarde est un point qui relève de la plus haute importance car elle participe à la conservation du savoir-faire. La sauvegarde informatique constitue la première action mais afin qu'elle soit efficace, elle doit être idéalement quotidienne et l'administrateur informatique doit s'assurer qu'elle soit correctement effectuée et que son rétablissement fonctionne. Dans un second temps, il faut sécuriser les supports de sauvegarde en privilégiant leur délocalisation dans un lieu sécurisé au maximum.

Minimiser les risques de pertes de données est tout aussi important que leur sauvegarde. Une solution de récupération des données au moyen d'un serveur clone par exemple constitue l'un des moyens le plus sûr de récupérer les données archivées en cas de perte. Il existe aussi des méthodes de sauvegarde qui permettent d'optimiser la quantité de stockage et de réduire au maximum les pertes en cas de panne matériel.

Une fois toutes ces propositions mises en place, « AutoConcept » aura un outils informatique optimal et optimisé. Comment restaurer un climat de confiance avec l'équipe informatique ou dans le cas la société qui gèrera le parc ?

6 La charte « Qualité Service client »

6.1 De façon générale

Chez JASSUR Informatique :

- Chaque intervention est personnalisée et se fait dans le respect des lois en vigueur.
- Tout personnel de JASSUR Informatique est identifiable facilement et sera toujours en mesure de prouver son identité.
- Chaque demande est prise en charge dans les meilleurs délais pouvant aller du jour même à quelques jours suivant la difficulté de votre demande.
- Toutes vos demandes génèrent un ticket d'intervention, qui permettra un meilleur suivi de nos techniciens et d'être plus réactifs face à vos sollicitations.
- Les interventions font l'objet d'un devis précis et d'une facture détaillée.
- Une fiche d'intervention est générée [Annexe 5](#) et un exemplaire vous est remis par mail.
- JASSUR Informatique étudie et adapte son fonctionnement en fonction des réclamations reçues [Annexe 6](#).

JASSUR Informatique hiérarchise les demandes suivant leurs retentissements sur le fonctionnement de la société.

- Demandes de haute importance : incidence empêchant le bon fonctionnement ou le fonctionnement même de la société liée aux prestations de JASSUR Informatique
- Demande importante : incident limitant le fonctionnement standard de la société mais sans impact majeur.
- Demandes peu importantes : pas de retentissement sur le fonctionnement de la société et nécessitant un temps de réflexion.

Cette répartition permettra d'organiser et de faire ressortir l'urgence des tickets d'incident. Nous pourrons répondre au plus vite à votre attente. Demande de haute importance prise en charge dans l'heure, demande importante dans la demi-journée et demande peu importante dans la journée.

JASSUR Informatique souhaite mettre l'accent sur trois points particuliers pour « AutoConcept » afin de rétablir le climat confiance entre le client et le service informatique :

- La continuité de service en cas de panne.
- Le relationnel client.
- La sécurité et la productivité.

6.2 La continuité de service en cas de panne.

JASSUR Informatique s'engage à :

- Une astreinte téléphonique joignable du lundi au samedi de 08h00 à 19h00.
- Un délai d'intervention sur site le jour même après diagnostic téléphonique pour analyser la situation et y apporter une solution.
- Si du matériel doit être emporté chez JASSUR Informatique, un matériel de secours pourra vous être fourni avec un minimum de fonctionnalités.
- Une sauvegarde automatique des données générées par les collaborateurs de la structure AutoConcept pourra être disponible très rapidement.
- La sauvegarde des fichiers sur un créneau nocturne permettant de récupérer les données perdues de moins de 24 heures sera installée dans un second temps.

Pour avoir un service de qualité, il faut aussi un relationnel client irréprochable.

6.3 Le relationnel client.

Quoi de plus normal que d'avoir un climat de confiance entre une société et son prestataire de service.

JASSUR Informatique a dans son ADN la qualité, et notamment la relation client à chaque intervention d'assistance informatique

L'accueil

Parce que chaque partenaire est différent, nous nous adaptons à ses besoins, nous nous adaptons à chaque interlocuteur. L'implication est un maître-mot, le ton est dynamique et chaleureux, sans oublier la politesse et le respect de la vie privée du client lors de chaque intervention.

L'écoute de vos attentes

Répondre aux attentes d'un partenaire commence par l'écouter et nos personnels reformulent afin de s'assurer qu'ils ont bien compris et utilisent un vocabulaire non-technique autant que possible. Différentes solutions peuvent être proposées afin de répondre au problème et la solution appliquée sera celle retenue par le client.

Le professionnalisme et le conseil

En nous basant sur un savoir-faire technique éprouvé, nous édifions la meilleure solution pour nos partenaires, nous les informons et conseillons en respectant une éthique professionnelle rigoureuse, en ayant à cœur de prendre en compte et de répondre aux objections.

Transparence et visibilité

Nos tarifications sont claires, toujours indiquées le plus clairement possibles avant intervention, en précisant en détail les opérations à effectuer. Nos opérations sont également prévues à l'avance, en accord avec nos partenaires pour permettre des opérations les plus fluides possibles.

L'engagement sur la durée

La satisfaction de nos partenaires est notre priorité, nous présentons toujours le cadre de la garantie avant intervention. Et bien sûr nous fournissons tous les documents afin que vous puissiez contacter le service après-vente si besoin.

A noter que ces différents éléments se retrouvent dans notre charte de service (SLA), en [Annexe 8](#)

7 Sécurité et productivité garantie par JASSUR Informatique

Une protection adéquate du matériel, des logiciels et des données est une réalité chez JASSUR Informatique pour cela, il sera effectué :

- Une gestion à distance de votre réseau informatique
- Une veille technologique régulière, le plan de veille en [Annexe 8](#)
- Une mise à jour régulière des logiciels et applications de l'entreprise via les licences officielles
- Une évaluation de sécurité des mots de passe
- Un choix de matériel optimal pour rester efficace pendant un minimum de trois ans
- Une maintenance du parc informatique et des logiciels de façon régulière
- Une installation des serveurs dans des locaux prévus à cet effet : climatisation, protection incendie, salle en surpression pour éviter la poussière, protection contre l'eau, et les locaux seront bien entendus sécurisés.

Cette charte sera donnée à « AutoConcept » en même temps que la proposition de JASSUR Informatique. Mais est-ce que nos engagements s'arrêtent là ?

Il faut aussi que JASSUR Informatique soit à la hauteur de ses promesses, que son image de marque soit bonne et que ses employés véhiculent aussi le savoir-faire et le savoir-être.

Afin que chaque salarié de JASSUR Informatique ancien ou nouveau sache ce que la société attend de lui, il lui sera remis un mémo sur la conduite à tenir chez le client.

8 Proposition de mémo sur la conduite à tenir chez un client.

Mémo pour tous les employés de JASSUR Informatique

Nous tenons à vous rappeler que vous êtes les **vecteurs de l'image de notre société** que ce soit en interne ou en externe.

Un exemplaire pour le salarié et un pour la direction

Il sera attendu de votre part :

Tenue correcte
Avoir toujours un moyen d'identification personnelle et professionnelle sur soi
Attitude professionnelle adéquate
Langage adapté et compréhensible par les clients
Être à l'écoute de ses collègues et des clients
Informer le client des aléas rencontrés
Ponctualité tant sur site que chez les clients
Respect des règles de politesse
Respect du secret et de la discrétion professionnelle
Respect des délais d'intervention
Respect des plannings dans la mesure du possible
Avoir l'esprit d'équipe et d'initiative
Remplir la fiche de suivi d'intervention
Suivi de la veille technologique
Respect des distances sociales et des gestes barrières
Prévenir le client et avoir l'accord avant toute interventions

Je soussigné(e)m'engage à honorer les différents points stipulés précédemment.

Fait à, le

Signature du salarié

Signature de la direction

9 Conclusion

« AutoConcept » souhaite améliorer la gestion de son parc informatique avec une refonte de son service informatique.

Quelles étaient ses besoins et les solutions apportées par JASSUR Informatique ?

- Lenteur de certains postes, vérification de la connexion internet, remise à niveau de ces ordinateurs.
- Message intempestif « version de Windows pirates », installation d'un seul système d'exploitation officiel, uniformisation des logiciels tous avec licences et mises à jour faites régulièrement.
- Intrusion d'un client, création de session utilisateur et de mot de passe.
- Crash disque d'un poste, création de moyens de sauvegarde. De façon immédiate instauration d'une sauvegarde journalière puis dans un second temps duplication de celle-ci. Tous cela sera fait avec sécurisation des locaux contenant les serveurs.
- Un utilisateur signale que MSN ne fonctionne pas, élaboration d'une charte informatique utilisateur, information et formation de ces derniers avec un listing des sites non autorisés chez « AutoConcept ».
- Un informaticien des deux informaticiens sera recruté par JASSUR Informatique. Il sera formé et devra appliquer le mémo de JASSUR Informatique. De plus, il aura en charge votre dossier, cela permettra de bénéficier de son expertise.
- Poste parti trop longtemps en SAV, fourniture de matériel de prêt.
- La fiche d'intervention, fournie par JASSUR Informatique et contresignée par vos soins, sera garante de la résolution de votre problème et du non-remplacement de matériel non prévu.
- Pour chaque demande de votre part, il y aura création d'un ticket d'intervention qui permettra de hiérarchiser le degré d'urgence de la prise en charge, afin d'avoir une meilleure réactivité.

Chaque partenaire sera pris en charge par un seul chef de projet et un technicien référent.

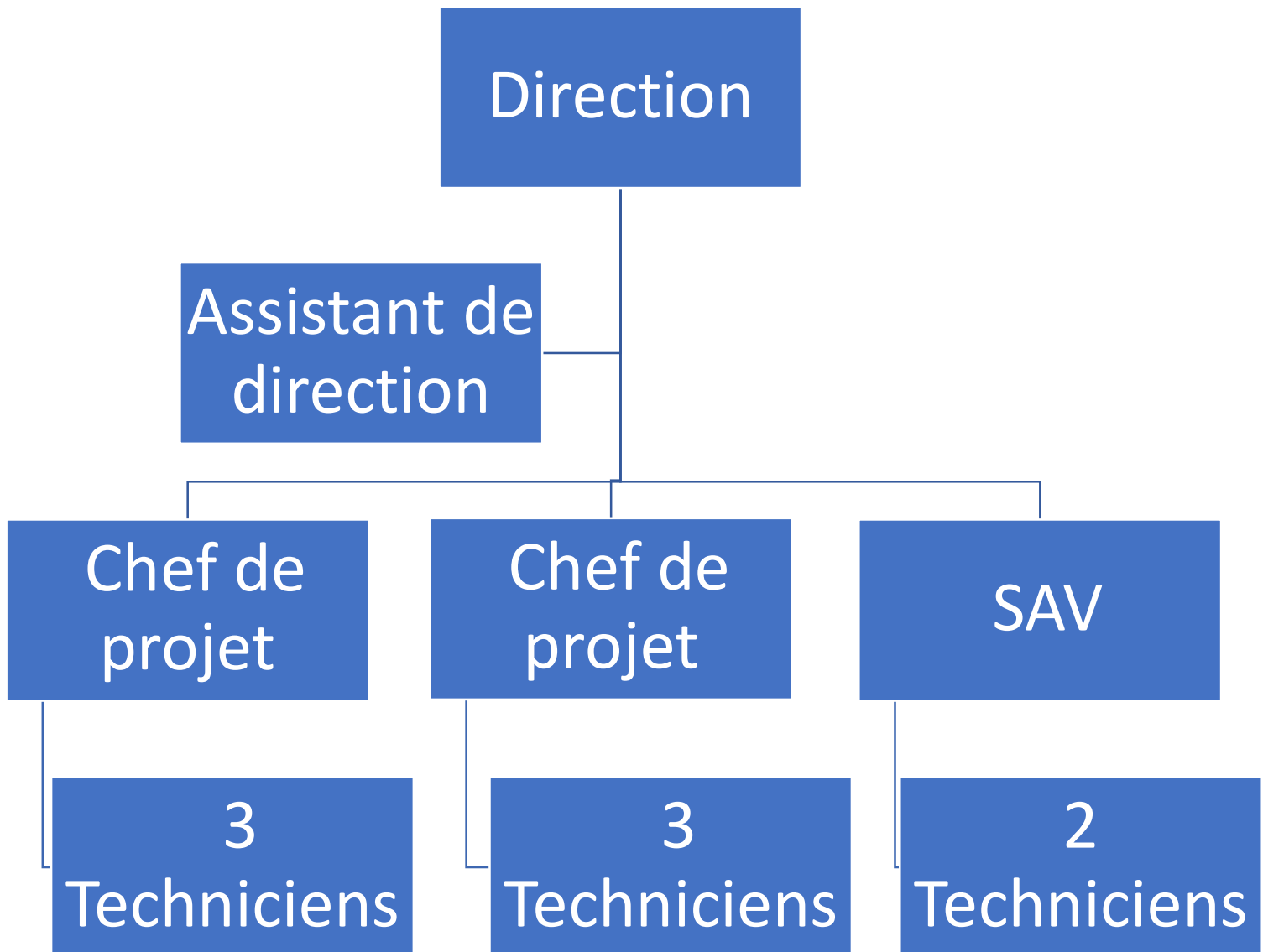
JASSUR Informatique répond en tous points à votre cahier des charges.

Pour la suite, nous vous proposons une rencontre entre notre directeur, votre chef de projet et vous-même afin de discuter des différentes solutions possibles et de vous détailler le devis qui en découle.

JASSUR Informatique propose un bilan à un an, en plus des fiches qualités à remplir à chaque intervention.

JASSUR Informatique reste à votre disposition pour tous renseignements complémentaires et attend avec impatience de pouvoir travailler avec vous.

10 Annexe 1 : Organigramme de JASSUR Informatique



11 Annexe 2 : Charte graphique de JASSUR Informatique

Couleurs utilisées

- **Bleu Foncé**
HEX 283785
RGB 40 55 133
- **Bleu Clair**
HEX 2270b8
RGB 34 112 184
- **Orange**
HEX e47925
RGB 228 121 37



TYPOGRAPHIE

Calibri

Il peut être utilisé **en gras**, *en italique*

Taille des caractères

Titre : 20

Titre 1 : 16

Titre 2 : 14

Texte : 11

Utilisation

Ne peut pas être mis sur un autre fond qu'un fond blanc
Respecter un cadre d'exclusion autour du logo



Pour une carte de visite

Créer un cadre bleu foncé et écrire dedans en blanc



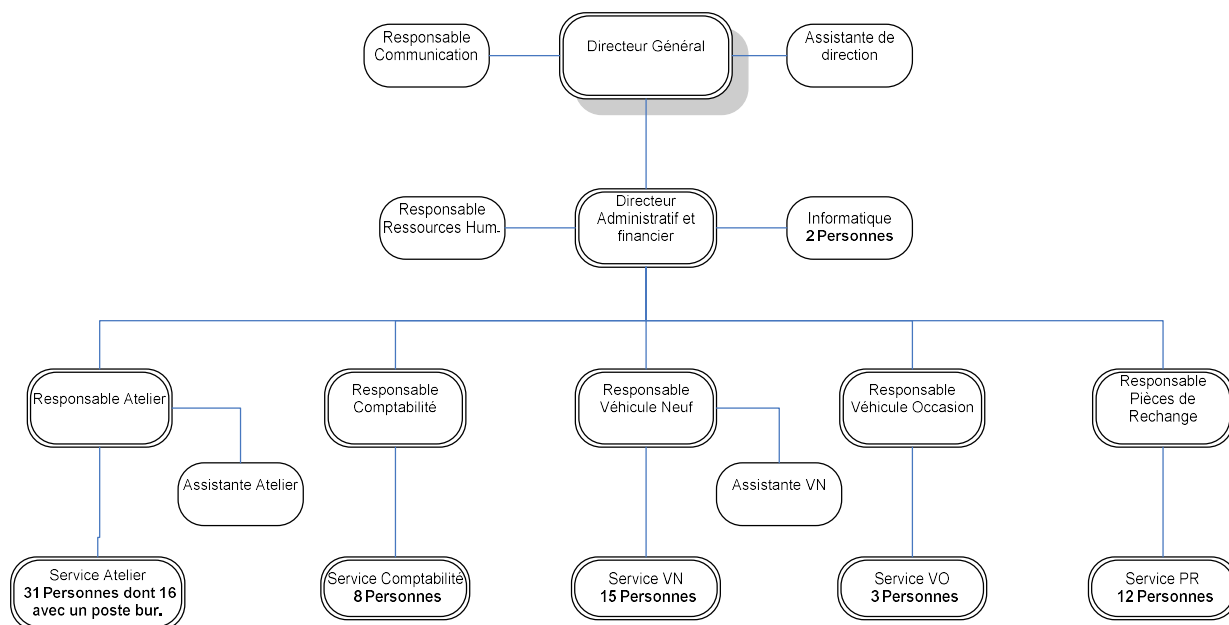
Rédaction d'un document

Marges standards 2,5 cm haut, bas, droite et gauche

En tête : logo de la société à droite

Pied de page : coordonnées de la société

12 Annexe 3 : Organigramme « AutoConcept »



13 Annexe 4 : Compte rendu du service commercial de « AutoConcept »

La société « AutoConcept » a choisi d'amortir son matériel sur 3 ans. La chef comptable est très réticente à tout renouvellement avant la fin de la période d'amortissement.

Lenteur de certains postes.

Crash disque du poste d'un commercial : perte d'exploitation 80 000 euros.

Intrusion d'un client sur un poste d'une commerciale dépourvu de mot de passe

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 une affaire. Perte : 60 000 euros.

Attitudes des techniciens : absence d'explication sur les interventions, ou parfois discours trop techniques

Messages intempestifs de « version de Windows pirates »

Tenue des informaticiens : « un matin, l'un d'eux est arrivé en jogging pour dépanner un poste alors qu'un commercial était avec un client ». Un autre a répondu de manière déplacée à la demande d'un utilisateur de le dépanner.

Une intervention urgente planifiée pour le lundi 10h a été traitée le mercredi à 10h.

Un utilisateur du service commercial se plaint que son poste, après plusieurs séjours au SAV, présente toujours les mêmes symptômes.

Un utilisateur de la comptabilité soupçonne le SAV d'avoir consulté des documents confidentiels sur son poste lors d'une intervention. Ces informations ont été divulguées à des tiers.

Un utilisateur de l'atelier rapporte qu'il a dû insister auprès du service informatique pour retrouver son écran d'origine. Un écran plus petit lui avait été remis après une intervention.

Un utilisateur du service « Véhicules d'occasion » se plaint depuis plusieurs mois d'avoir des problèmes avec sa souris. Personne n'a répondu à son problème.

Plusieurs utilisateurs se plaignent de l'accueil téléphonique du service informatique.

Une bonne partie des utilisateurs se plaignent de voir leurs postes partir en SAV sans savoir quand il reviendra.

Un utilisateur signale que son MSN ne fonctionne pas et souhaite que son poste soit réparé rapidement. (NB : la direction a demandé au service informatique de bloquer MSN. Depuis la productivité a considérablement augmentée).

14 Annexe 5 : Textes de loi

Lois et textes relatifs à l'utilisation de l'informatique dans une entreprise :

Création de la Cnil informations

Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés


[> Loi Informatique et Libertés](#) 

[> Sanctions pénales](#) 

[> Textes d'application](#) 

Texte référence

Directive européenne n°95/46/CE du 24 octobre 1995

[> Directive européenne n°95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.](#) 

Texte référence

Charte des droits fondamentaux de l'Union européenne

[> Le texte intégral de la Charte \(version française\)](#) 

[> Chapitre II : libertés](#) 

Texte référence

Convention 108

[> Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel](#) 

[> Protocole additionnel](#)

Loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles

NOR: JUSC1732261L

ELI: <https://www.legifrance.gouv.fr/eli/loi/2018/6/20/JUSC1732261L/jo/texte>

Alias: <https://www.legifrance.gouv.fr/eli/loi/2018/6/20/2018-493/jo/texte>

L'Assemblée nationale et le Sénat ont délibéré,

L'Assemblée nationale a adopté,

Vu la décision du Conseil constitutionnel n° 2018-765 DC du 12 juin 2018 ;

Le Président de la République promulgue la loi dont la teneur suit :

Titre Ier : DISPOSITIONS D'ADAPTATION COMMUNES AU RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016 ET À LA DIRECTIVE (UE) 2016/680 DU PARLEMENT EUROPÉEN ET DU CONSEIL DU 27 AVRIL 2016

Loi n° 92-597 du 1 juillet 1992 relative au code de la propriété intellectuelle (partie législative)
NOR : MENX9100082L
Version consolidée au 08 juillet 2020

Article 1 [En savoir plus sur cet article...](#) : Les dispositions annexées à la présente loi constituent le code de la propriété intellectuelle (partie Législative).

Article 2 [En savoir plus sur cet article...](#) : Les références contenues dans les dispositions de nature législative à des dispositions abrogées par l'article 5 de la présente loi sont remplacées par des références aux dispositions correspondantes du code de la propriété intellectuelle.

Article 3 : Les dispositions du code de la propriété intellectuelle (partie Législative) qui citent en les reproduisant des articles d'autres codes sont de plein droit modifié par l'effet des modifications ultérieures de ces articles.

Article L1121-1 du code du travail

« Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché »

Article L432-2-1 du code du travail

Modifié par [Loi n°2001-152 du 19 février 2001 - art. 1 JORF 20 février 2001](#)

Abrogé par [Ordonnance n°2007-329 du 12 mars 2007 - art. 12 \(VD\) JORF 13 mars 2007 en vigueur au plus tard le 1er mars 2008](#)

Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de ceux-ci.

Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci.

Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés.

NOTA :

Ordonnance 2007-329 2007-03-12 art. 14 : Les dispositions de la présente ordonnance entrent en vigueur en même temps que la partie réglementaire du nouveau code du travail et au plus tard le 1er mars 2008.

La loi n° 2008-67 du 21 janvier 2008 dans son article 2 X a fixé la date d'entrée en vigueur de la partie législative du code du travail au 1er mai 2008.

Lois et textes relatifs au filtrage dans une entreprise :

Décision n° 1151/2003/CE du Parlement européen et du Conseil du 16 juin 2003 modifiant la décision n° **276/1999/CE** adoptant un plan d'action communautaire pluriannuel visant à promouvoir une utilisation plus sûre d'Internet par la lutte contre les messages à contenu illicite et préjudiciable diffusés sur les réseaux mondiaux. (JO L 162 du 1er juillet 2003) (Notification d'adoption publiée au JOLD du 04/07/2003 p.11363

Contenu et portée :

Le plan d'action adopté en 1999 comporte trois lignes d'action principales :

- créer un environnement plus sûr (en particulier grâce au « réseau européen de lignes directes », reposant sur des permanences téléphoniques auxquelles le public peut signaler les contenus illicites et grâce à la fourniture de conseils pour la mise en œuvre de codes de conduite) ;
- développer les systèmes de filtrage et de classification ;
- encourager les actions de sensibilisation.

Ce dispositif a donc un objet essentiellement pratique et non pas juridique (d'autres initiatives ont été prises par la Communauté européenne et par le Conseil de l'Europe sur ce dernier terrain).

Au total, 35 projets devraient être financés par ce plan d'action quadriennal.

Sa prolongation de deux années permettrait surtout :

- d'étendre le champ des technologies couvertes : l'accent ne serait plus mis uniquement sur le contenu du web, mais également sur l'accès mobile et à large bande au contenu, les jeux en ligne, le transfert de fichiers de poste à poste et toutes formes de communication en temps réel (les « salons de bavardage ») ;
- d'élargir le champ des thèmes couverts : la lutte serait menée non seulement contre la pornographie infantile, et pour la protection des mineurs, mais également contre le racisme, la violence...

Loi n° 2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

NOR : INTX0500242L

Version consolidée au 08 juillet 2020

[Recommandation CM/Rec\(2008\)6 du Comité des Ministres aux Etats membres sur les mesures visant à promouvoir le respect de la liberté d'expression et d'information au regard des filtres internet adoptée le 26 mars 2008](#)

[Recommandation Rec\(2001\)8 du Comité des Ministres aux Etats membres sur l'autorégulation des cyber-contenus \(l'autorégulation et la protection des utilisateurs contre les contenus illicites ou préjudiciables diffusés sur les nouveaux services de communication et d'information\) adoptée le 5 septembre 2001](#)

[Recommandation CM/Rec\(2007\)11 du Comité des Ministres sur la promotion de la liberté d'expression et d'information dans le nouvel environnement de l'information et de la communication adoptée le 26 septembre 2007](#)

Directive 2002/58/CE du Parlement européen et du Conseil 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)

Journal officiel n° L 201 du 31/07/2002 p. 0037 – 0047 <http://data.europa.eu/eli/dir/2002/58/oj>

LOI no 92-684 du 22 juillet 1992 portant réforme des dispositions du code pénal relatives à la répression des crimes et délits contre les personnes (1)

JORF n°169 du 23 juillet 1992 page 9857

NOR : JUSX8900010L

L'article 9 alinéa 1 du code civil dispose que : « Chacun a droit au respect de sa vie privée. » Ainsi, chacun a, sur le fondement de l'article 9 du code civil, le droit de s'opposer à la reproduction de son image ou la diffusion de tout commentaire relatif à sa vie privée.

Arrêt du 5 septembre 2017

<http://hudoc.echr.coe.int/fre?i=001-177083>

Article L121-8

Créé par [Loi n°92-1446 du 31 décembre 1992 - art. 26 JORF 1er janvier 1993](#)

Abrogé par [Ordonnance n°2007-329 du 12 mars 2007 - art. 12 \(VD\) JORF 13 mars 2007 en vigueur au plus tard le 1er mars 2008](#)

Aucune information concernant personnellement un salarié ou un candidat à un emploi ne peut être collectée par un dispositif qui n'a pas été porté préalablement à la connaissance du salarié ou du candidat à un emploi.

NOTA :

Ordonnance 2007-329 2007-03-12 art. 14 : Les dispositions de la présente ordonnance entrent en vigueur en même temps que la partie réglementaire du nouveau code du travail et au plus tard le 1er mars 2008.

La loi n° 2008-67 du 21 janvier 2008 dans son article 2 X a fixé la date d'entrée en vigueur de la partie législative du code du travail au 1er mai 2008.

Article L1121-1 [En savoir plus sur cet article...](#)

Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Arrêt du 9 juillet 2008 de la cour de Cassation

Analyse

Publication : Bulletin 2008, V, n° 150

Décision attaquée : Cour d'appel de Nancy , du 27 septembre 2006


Titrages et résumés : CONTRAT DE TRAVAIL, EXECUTION - Employeur - Pouvoir de direction - Étendue - Contrôle et surveillance des salariés - Recherche des connexions établies par un salarié sur des sites internet - Conditions - Portée

Les connexions établies par un salarié sur des sites internet pendant son temps de travail grâce à l'outil informatique mis à sa disposition par son employeur pour l'exécution de son travail sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier, hors de sa présence

PROTECTION DES DROITS DE LA PERSONNE - Respect de la vie privée - Atteinte - Défaut - Cas - Recherche par l'employeur des connexions établies par un salarié sur des sites internet - Conditions - Portée

Précédents jurisprudentiels : Sur la présomption du caractère professionnel du contenu informatique de l'ordinateur mis à la disposition du salarié, à rapprocher : Soc., 18 octobre 2006, pourvoi n° 04-48.025, Bull. 2006, V, n° 308 (rejet)

15 Annexe 6 : Enquête de satisfaction



Enquête de satisfaction

Madame, Monsieur nous venons de travailler ensemble, nous sommes dans une démarche de qualité.
Pourriez-vous remplir ce questionnaire afin de nous permettre de nous améliorer ?

Votre nom :

Votre entreprise : Date de l'intervention :

		Très satisfait	Satisfait	Peu satisfait	Pas satisfait
Prise de rendez-vous	L'accueil téléphonique et/ ou physique	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Facilité pour la prise de contact	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Ponctualité	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	A votre écoute	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Conseil	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Langage adapté	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Professionalisme	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Devis et facture	Rapidité d'obtention	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Devis inscrit clairement	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Devis expliqué	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Prix	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Facture conforme au devis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Intervention	Respect du devis	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Respect des horaires	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Respect des délais prévus	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Professionalisme de l'intervenant	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Propreté du chantier	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Qualité du matériel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Intervention à la hauteur des attentes	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	De façon global	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Commentaires :

.....


.....

Merci de votre collaboration

JASSUR Informatique

7 bis Avenue Robert Schuman, 51100 Reims

16 Annexe 7 : Fiche d'intervention JASSUR Informatique



JASSUR INFORMATIQUE

FICHE D'INTERVENTION JASSUR Informatique

Nom de la société :	Nom du responsable :
Adresse :	Téléphone :
Complément adresse :	

Nom du contact :	Contrat : <input type="checkbox"/> OUI <input type="checkbox"/> NON
------------------------	---

Nom du technicien : Choisissez un élément.	Date : Cliquez ou appuyez ici pour entrer une date.	Heure d'arrivée :
Signature du technicien :	Signature du client :	

Description :

Nouveaux matériels installés :

Commentaires / Observations :

Jour et Heure de fin :	Remarques clients :	Signature du client :
---	--	-------------------------------

JASSUR Informatique
 7 bis Avenue Robert Schuman, 51100 Reims
 jassurinformatique@viacesi.fr SAV : 06 86 LA MG NB

17 Annexe 8 : Proposition de Contrat SLA

Projet SAS


JASSUR INFORMATIQUE

Juillet 2020

CONTRAT SERVICE LEVEL AGREEMENT (SLA)

Contrat-cadre N°1

Relatif au service SLA pour services informatiques
Entre la Société **JASSUR informatique** et **AutoConcept**

Objectif du présent document

L'objectif du présent document consiste à définir le cadre de prestations informatiques fournis à AutoConcept.

JASSUR informatique s'engage à :

Sur la base du présent contrat-cadre, JASSUR informatique fourni au AutoConcept des prestations dans le domaine du traitement d'informations techniques et commerciales, éventuellement combinées avec la livraison de logiciels ou de matériels qui sont en rapport avec les prestations. JASSUR informatique note que, de son côté, AutoConcept s'engage à respecter les accords contractuels conclus entre nos deux entités.

AutoConcept s'engage à :

AutoConcept représente la partie acceptant une certaine prestation de JASSUR informatique, fournisseur de prestations. Le catalogue de prestations est déterminé en fonction de ses besoins.

Les accords suivants constituent le contrat-cadre. Une obligation concrète liant les parties ne naît que sur la base d'une convention particulière figurant dans une annexe et/ou dans une commande d'AutoConcept.

Jusqu'au moment de la conclusion, établie d'une signature d'une convention correspondante, les deux parties peuvent se retirer des négociations sans qu'il y ait des conséquences financières. Sauf accord particulier, AutoConcept ne doit pas prendre à sa charge les coûts relatifs à des activités déjà effectuées par JASSUR informatique telles que des activités marketing, des recherches particulières, des consultations, la préparation d'offres ainsi que des frais de voyages et autres frais professionnels.

Signature JASSUR informatique :

Signature AutoConcept :

JASSUR Informatique

7 bis Avenue Robert Schuman, 51100 Reims

18 Annexe 9 : Plan de Veille

Plan de veille de « AutoConcept »

Besoins	Objectifs	Fréquence	Destinataires	Source/outils	Livrables
Parc vieillissant : évolution du parc	+meilleure productivité. Plus continuité de service Plus de confort	Trimestrielle	Directeur de « AutoConcept » Technicien	Web Fournisseur Revues Conférences Benchmark	Mail Rapport écrit Note d'information Comparatif versus actuel
Surveillance de l'OS	Protection du système	Quotidienne	Technicien	Ansii Web	Mail
Sauvegarde	Protection des données	Quotidienne	Technicien	Expert	Mail
Mot de passe	Protection des données	Mensuelle	Technicien	Web CNIL	Mail
Logiciel non officiel	Utilisation de licences fournies par le distributeur officiel	Mensuelle	DAF	Web Fournisseur Revues	Rapport écrit
Faible informatique	Meilleure protection	Mensuelle	Technicien	Web Revues	Mail
La législation	Être toujours à jour pour éviter les peines	Mensuelle	Technicien Direction	Légifrance CNIL	Mail Rapport écrit
Offre internet	Meilleure offre	Trimestrielle	Direction	Site des FAI	Mail

19 Annexe 10 : Gestion de projet

Note de synthèse :	Règlement utilisation des moyens informatiques à disposition des salariés	Bénédicte Gérard Alex Matthieu
	La sécurité des fichiers (quels moyens ?)	
	Les informations sur les outils informatiques	
	Solution de filtrage (dispositions légales)	
Plan de sécurisation des données :	Sécurité de mot de passe	Alex Matthieu
	Sauvegarde immédiate	
Charte « Qualité Service Client » :	Généralités	
	Continuité de service en cas de panne	
	Relationnel client	
	Sécurité/productivité	
Mémo :	Conduite à tenir	
Conclusion :	Conclure sur le projet	

20 Notre ressenti

Le projet SAS a permis de se faire une idée concrète des problématiques rencontrées chez le client dans le cadre d'une prestation et d'en déduire les réflexes à acquérir en qualité de technicien informatique.

Il est en effet important dans un premier temps de s'imprégner du contexte professionnel du client et d'en définir ses besoins.

Réaliser un audit technique afin d'analyser l'état de son parc informatique.

En déduire ensuite les solutions potentielles qui pourraient être envisagées et établir une proposition au client. Cette dernière présentera les différentes solutions possibles, le tout pour optimiser le parc informatique et l'utilisation de ses périphériques par les intervenants au sein de la structure.

Nous avons pu prendre conscience de l'importance de la sécurisation du réseau aussi bien du point de vue matériel que des données stockées et de leurs sauvegardes.

Il a fallu prendre en considération les lois en vigueur, se documenter aussi bien sur les droits d'actions pour encadrer au mieux l'utilisation de l'outils numérique que sur ses devoirs en matière de préservation des données. Ces dernières sont relatives au savoir-faire de l'activité. Il a fallu aussi porter l'accent sur les données personnelles des salariés ainsi que sur la limite du champ d'actions de manière à respecter la vie privée de chacun.

Cette introduction au métier de technicien des supports informatiques a été un projet enrichissant qui a permis d'envisager la suite de notre formation et les sujets qui pourront y être abordés.

21 Glossaire

ANSSI : Agence nationale de la sécurité des systèmes d'information

CE : Communauté Européenne

CEDH : Cour européenne des droits de l'homme

CNIL : Commission nationale de l'informatique et des libertés

CPI : Cour pénale internationale

DAF : Directeur des Affaires Financières

DCP : données à caractère personnel. Toutes informations se rapportant à une personne physique identifiable ou identifié

DPO : Data Protection Officer

FAI : Fournisseur d'accès à Internet

GMSI : Gestionnaire en maintenance et support informatique

JO : Journal Officiel

JORF : Journal Officiel de la République Française

LCEN : La loi pour la confiance dans l'économie numérique

NAS : Network Attached Storage ou boîtier de stockage en réseau

NOR : système normalisé de numérotation des textes officiels français

OS : Système d'exploitation

PME : Petite ou moyenne entreprise

RGPD : Règlement général sur la protection des données

SLA : Service Level Agreement

TPE : Très petite entreprise

22 Bibliographie

<https://www.cnil.fr/fr/10-conseils-pour-la-securite-de-votre-systeme-dinformation>

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

www.coe.int

eur-lex.europa.eu

GUIDE DES BONNES PRATIQUES DE L'INFORMATIQUE : *12 règles essentielles pour sécuriser vos équipements numériques* de cpme confédération de pme

La charte Qualité M.C.I INFORMATIQUE

Livre blanc juridique Olfeo co-écrit avec le cabinet d'avocats Alain Bensoussan

https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf