GUILLAUME HARDY
GEFFIER PIERRE-EMMANUEL

PROJET SAS

Table des matières

INTRODUCTION ET PRESENTATION

I. PRESENTATION DE L'ENTREPRISE

A. Histoire de la société

HOTH INFO est une SARL au capital social de 50000 euros qui a été créée par son directeur actuel, en 2000. Initialement associé avec un des techniciens de l'entreprise, ils ont su gagner et garder la confiance de leurs clients ce qui leur permit un développement rapide et durable.
Aujourd'hui composée de huit techniciens, de deux ingénieurs, d'un responsable commercial, d'une assistante de direction et du directeur, HOTH INFO peut s'inscrire dans des relations clientes de qualité. Les compétences de ses employés sont un gage d'efficacité pour tous ses partenaires.

B. Coordonnées

HOTH INFO
ZI du PINSAN
26 RUE J.Baptiste PERRIN
33326 Eysines
Tel : 05.57.62.31.87 Fax : 05.57.62.31.86


C. Secteur d'activité

HOTH INFO est une société de services informatiques qui assure aussi bien des prestations au sein de ses entreprises clientes que des partenariats d'infogérance à distance depuis les locaux situés dans la zone industrielle d'Eysines. Effectuant des prestations pour de grands groupes comme la Banque Populaire ou le Groupe Bordeaux Nord Aquitaine Polyclinique, nous sommes également attentifs au besoin de structures plus modestes (PME,PMI) afin de répondre à tout type de besoins.

Nos prestations :

- **Infrastructure :**
  - Déploiement de parc informatique.
  - Maintenance et support.
  - Infogérance.
- **WEB :**
  - Développement de sites web.
- **Relation client :**
  - Consulting en technologie et stratégie.
  - Formation en entreprise.

Nos partenaires :

Microsoft

D. Quelques-uns de nos clients

Groupe Bordeaux Nord Aquitaine Polyclinique

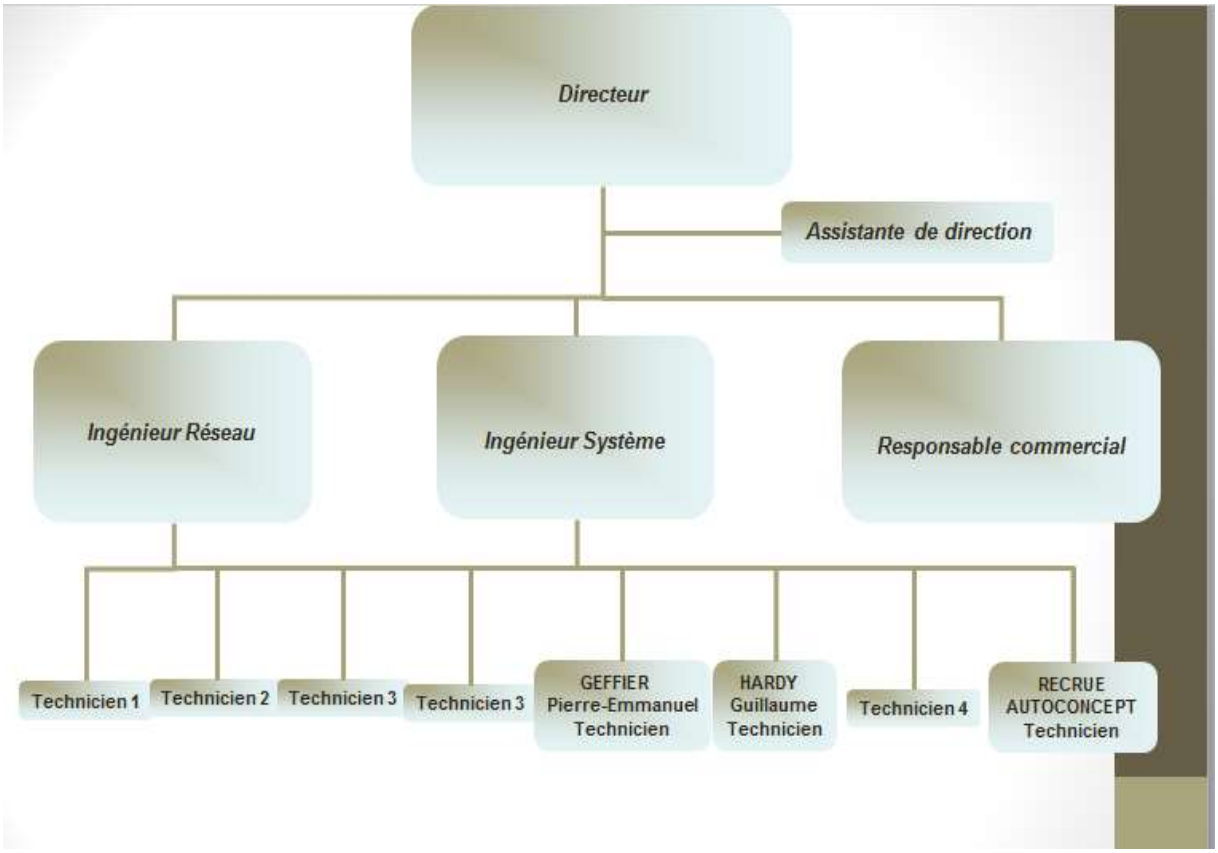
Banque Populaire

Cabinet d'avocats LEXCO

Campus de BISSY

E. Notre Equipe

1. Organigramme



2. Nos Compétences

- Ingénieur Réseau :
  - Titre de niveau II « Responsable en ingénierie réseaux » au CESI Blanquefort en 2005
  - Certifications : CISCO CCNA et CCNP
- Ingénieur système :
  - Titre de niveau I à l'EPSI de Bordeaux
  - Certifications : MCTS, MCITP, MCDST et MCSE
- Techniciens :
  - Minimum Diplôme ou titre de niveau III en informatique
  - Gestion de maintenance informatique
  - Technicien réseaux informatiques
  - Développeur web
- Responsable Commercial
  - BTS Management des unités commerciales en 2000
- Assistante de direction :
  - BTS Assistant de Manager en 2003

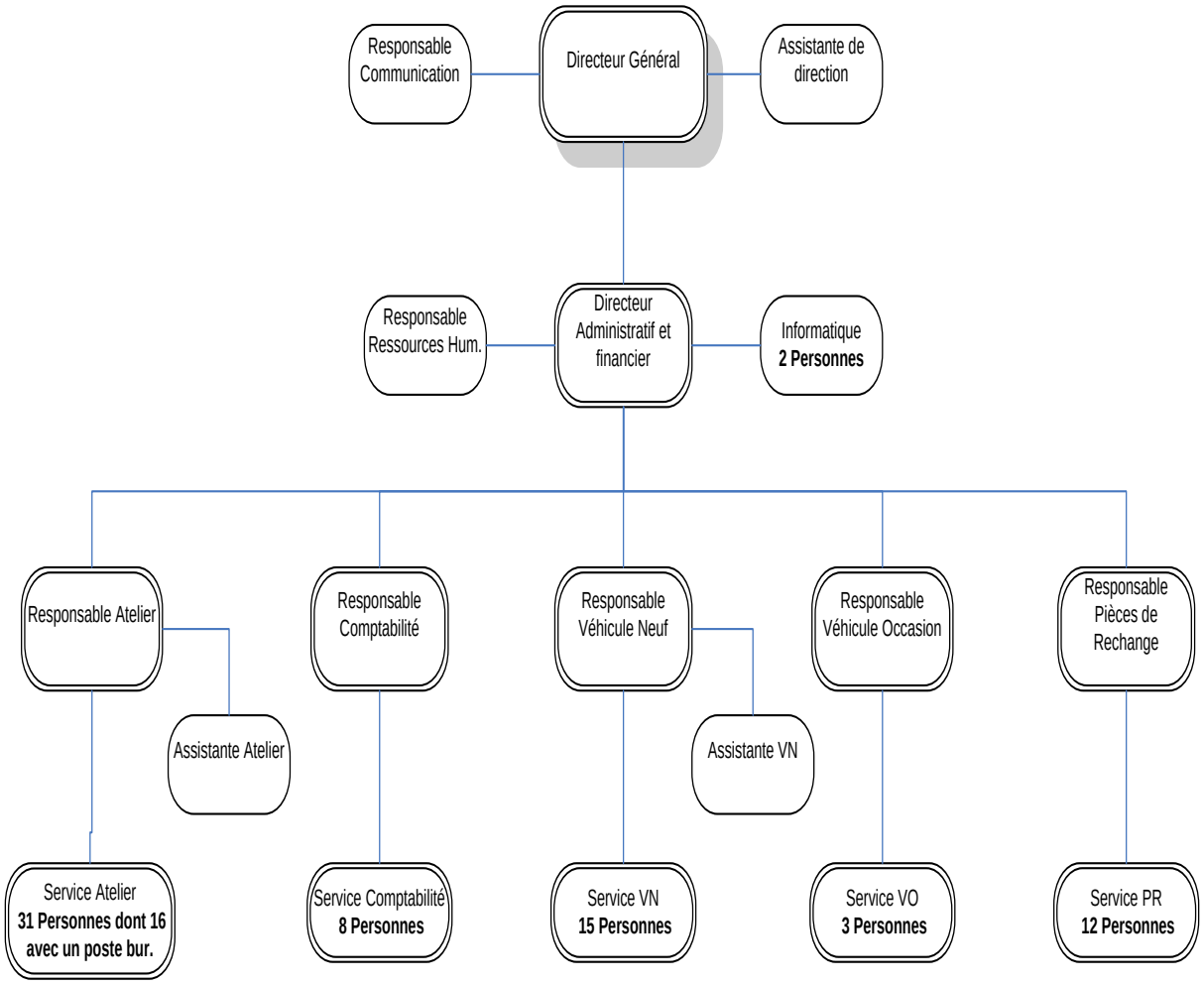
II. PRESENTATION DE L'APPEL D'OFFRE SAS

F. L'entreprise Autoconcept

Autoconcept est un concessionnaire automobile ayant des activités de vente de voitures neuves et d'occasions, de réparation et d'entretien d'automobiles.

Suite à une gestion catastrophique de son parc informatique et devant l'accumulation des problématiques dans ce domaine, l'entreprise Autoconcept a décidé d'externaliser les prestations informatiques actuellement exécutées par ses deux informaticiens.

Son parc informatique comprend actuellement 66 postes fixes, 4 ordinateurs portables, 1 serveur et 8 services d'impression.



G. Etude réalisée

Dans le cadre de l'appel d'offre de l'entreprise Autoconcept, nos directeurs nous ont demandé de réaliser une étude permettant à la fois de répondre au mieux à celui-ci et de

mettre à jour certaines connaissances et certains documents qu'utilisera par la suite notre entreprise HOTH INFO.

Nous avons donc réalisé :

- Une étude des principaux fondements légaux de l'utilisation des moyens informatiques.
- L'élaboration d'un plan de sécurisation des données à l'intention d'Autoconcept.
- Une Charte « Qualité Client Service ».
- Un mémo de rappel des bonnes pratiques à l'intention de tous les membres de HOTH INFO.

Nous présentons des documents tels que :

- Une nouvelle charte informatique pour Autoconcept
- Un schéma des bonnes pratiques d'un technicien de maintenance informatique
- Un schéma d'une bonne gestion des appels téléphoniques
- Une présentation de notre plateforme de ticketing des incidents informatiques

PREMIERE PARTIE : Note de synthèse sur les problématiques d'utilisation des outils informatiques en entreprise

I. REGLES REGISSANT L'UTILISTATION DES SYSTEMES INFORMATIQUES MIS A DISPOSITION DES SALARIES

A. Introduction

Le cadre légal des règles concernant l'utilisation des ressources informatiques repose sur trois fondements :
-La « loi relative à l'informatique, aux fichiers et aux libertés » établie en 1978.
-La Commission Nationale pour l'Informatique et les Libertés (CNIL).
-La charte informatique (propre à chaque entreprise).

1. La loi relative à l'informatique, aux fichiers et aux libertés

Elle a été établie en 1978 puis révisée régulièrement. Elle pose tout le cadre légal permettant de régir l'utilisation des outils informatiques et de prévenir tout abus, malveillance ou autres comportements susceptibles de porter atteinte aux libertés individuelles.

2. La CNIL

« La CNIL est l'autorité en charge de veiller à la protection des données personnelles. A ce titre, elle dispose notamment d'un pouvoir de contrôle et de sanction. Jouant aussi un rôle d'alerte et de conseil, elle a pour mission de veiller à ce que le développement des nouvelles

technologies ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

Ses missions :
-**Informer** les personnes sur leurs droits.
-**Protéger** les citoyens dans l'exercice de leurs droits.
-**Réguler** le traitement des données
-**Contrôler** que les responsables des systèmes d'information respectent la loi.
-**Sanctionner** les responsables des systèmes d'information ne respectant pas la loi.
-**Anticiper** les développements technologiques pour adapter ses politiques.

3. La Charte informatique

La charte informatique est un code de déontologie formalisant les règles légales et de sécurité relatives à l'utilisation de tout système d'information et de communication au sein d'une collectivité : applications métiers, bureautique, messagerie, micro-ordinateurs fixes et portables, périphériques, téléphones fixes et portables, Internet, Extranet, Intranet.

Une charte s'inscrit dans une démarche d'explication et de sensibilisation quant aux enjeux et aux risques. L'objectif est de faire adhérer les collaborateurs d'une entreprise afin de limiter les responsabilités pénales et civiles. Il faut donc que la charte soit claire et à la portée de tous.

B. Internet et Messagerie

1. Internet

La CNIL informe que : « L'employeur peut fixer les conditions et limites de l'utilisation d'internet. Ces limites ne constituent pas, en soi, une atteinte à la vie privée des salariés. »

Toutefois elle précise que ces limitations doivent être cohérentes avec l'activité professionnelle et le principe de liberté individuelle.

Les objectifs de ces limitations sont :

- D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie...).
- De limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux…).

L'utilisation d'internet est en principe réservée aux usages professionnels mais il est généralement admis qu'une utilisation personnelle peut être autorisée si celle-ci n'entrave pas l'activité professionnelle et si elle ne porte pas atteinte à certains principes de droit.

Le téléchargement, en tout ou partie, de données numériques soumis aux droits d'auteurs ou à la loi du copyright (fichiers musicaux, logiciels propriétaires, etc.) est strictement interdit.

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. La copie d'un logiciel constitue le délit de contrefaçon.

L'utilisateur ne doit pas porter atteinte à la propriété intellectuelle d'autrui, notamment via la reproduction, la représentation ou la diffusion d'une œuvre en violation des droits de l'auteur ou de toute autre personne titulaire de ces droits.

Certains contenus peuvent directement engager la responsabilité de l'utilisateur et de l'entreprise :

- Contenus pédopornographiques.
- Sites de jeux en ligne illégaux.
- Protection des droits d'auteur.
- Sites à caractères raciste, révisionniste.

En règle générale, l'entreprise établit sa politique en ce qui concerne sa politique d'accès à internet dans la charte informatique. Elle peut interdire ou autoriser certaines utilisations, comme par exemple l'utilisation de logiciels de messagerie instantanée ou l'accès aux réseaux sociaux.

Nous verrons par la suite que l'utilisateur a le droit à un espace privé, que ce soit pour des fichiers personnels, des courriels ou des sites internet. Cet espace doit être précisément identifié par la mention « privé » ou « personnel ».
En ce qui concerne internet, « les marque-pages, « favoris » ou « bookmark » du navigateur ne constituent pas un espace personnel ou privé. Ajouter un site internet à ses « favoris » ne limite donc pas le pouvoir de contrôle de l'employeur. »(CNIL)

Les moyens de contrôle de l'employeur seront précisés dans la partie « Filtrage de contenu »

2. La messagerie électronique

La CNIL définit de façon claire les aspects légaux de l'utilisation de la messagerie électronique :

« Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé ».

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées. Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles. Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :
- en précisant dans leur objet « Personnel » ou « Privé »
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriels ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.

« L'employeur doit respecter le secret des correspondances privées. Une communication électronique émise ou reçue par un employé peut avoir le caractère d'une correspondance privée. La violation du secret des correspondances est une infraction pénalement sanctionnée par les articles L.226-15 (pour le secteur privé) et L.432-9 (pour le secteur public) du Code pénal. »

Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages. En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé. »

C. Les fichiers personnels

1. Généralité

Dans son document « Les outils informatiques au travail », la CNIL nous informe que : « par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement. Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder :
-en présence de l'employé ou après l'avoir appelé.
-en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprécier ».

2. Fichier personnel, Mobilité, Absences, Départ

L'article 34 de la loi « Informatique et Libertés » explique que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Ainsi en cas, de départ ou d'absence d'un utilisateur, toutes les données présentes sur son poste informatique sont susceptibles d'être récupérées, lues voire utilisées si celles-ci présentent un intérêt pour l'entreprise.

Toutefois il est souhaitable que chaque utilisateur amené à quitter ses fonctions de façon temporaire ou définitive ne laisse sur son poste informatique que des données en lien avec son activité professionnelle.

En cas de vol d'un équipement informatique professionnel (ordinateur portable, téléphone portable…), l'utilisateur est dans l'obligation de le signaler au plus vite à l'administrateur réseau. Ce dernier, en concertation avec la direction, prendra toute les mesures nécessaires à cet égard (dépôt de plainte, blocage des accès au réseau…)

II. INFORMATION AUX SALARIES

D. Généralités

La CNIL dans son « Guide pour les employés et les employeurs » écrit :

« Conformément aux dispositions du code du travail (L2323-32) et aux textes relatifs aux trois fonctions publiques (**lois n°84-16 du 11 janvier 1984, n°84-53 du 26 janvier 1984 et n°86-33 du 9 janvier 1986**), les instances représentatives du personnel doivent être consultées et précisément informées des fonctionnalités envisagées dans le cas de mise en oeuvre de traitements qui ont une incidence sur le personnel.
De plus, le code du travail prévoit qu'aucune information concernant directement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance (L1221-9 et L1222-4).

Les employés doivent, dans tous les cas de figure, être informés individuellement de l'existence des traitements contenant des données personnelles les concernant par note, affichage, publication dans le journal interne, courrier électronique... En application de la **loi du 6 janvier 1978 modifiée**, les personnels concernés doivent être informés de la ou des finalité(s) et fonctionnalités précises de chaque traitement automatisé mis en œuvre par l'employeur, des conséquences individuelles qui pourront en résulter (par exemple un contrôle), des destinataires des données enregistrées et de leur droit d'accès, d'opposition et de rectification à ces données. À cet égard, la déclaration adressée à la CNIL doit préciser les mesures relatives à l'information individuelle des salariés. Toute personne peut obtenir communication de la liste des traitements déclarés au sein d'un organisme sur simple demande écrite (**article 31 de la loi du 6 janvier 1978 modifiée**). »

En pratique l'information passe prioritairement par le biais de la charte informatique. Celle-ci doit-être validée par les représentants du personnel, puis par le comité d'entreprise. Enfin pour les entreprises de plus de 20 salariés (où un règlement intérieur est obligatoire) elle peut être annexée au règlement intérieur une fois approuvée par l'inspection du travail.

E. Internet :

Les salariés doivent être informés des dispositifs mis en place et des modalités de contrôle de l'utilisation d'internet :

Le comité d'entreprise doit avoir été consulté et informé (article L2323-32 du code du travail). **Les salariés doivent être informés,** notamment **de la finalité** du dispositif de contrôle et **de la durée** pendant laquelle les données de connexion sont conservées. Une durée de conservation de l'ordre de six mois est suffisante, dans la plupart des cas, pour dissuader tout usage abusif d'internet.

Si des procédures disciplinaires sont susceptibles d'être engagées sur la base de ces fichiers, les salariés doivent en être explicitement informés (par exemple au moyen d'une charte).

Lorsque l'entreprise ou l'administration met en place un dispositif de contrôle individuel des salariés destiné à produire un relevé des connexions ou des sites visités, poste par poste, le traitement ainsi mis en œuvre doit être déclaré à la CNIL (déclaration normale) sauf si un correspondant informatique et libertés a été désigné, auquel cas aucune déclaration n'est nécessaire.

F. Messagerie :

Les dispositifs de contrôle de la messagerie doivent faire l'objet d'une consultation du comité d'entreprise ou, dans la fonction publique, du comité technique paritaire ou de toute instance équivalente et d'une information individuelle des salariés.

Ils doivent notamment être informés, de la finalité du dispositif et de la durée pendant laquelle les données de connexion sont conservées ou sauvegardées.

En cas d'archivage automatique des messages électroniques, ils doivent en outre être informés des modalités de l'archivage, de la durée de conservation des messages, et des modalités d'exercice de leur droit d'accès.

La messagerie professionnelle doit faire l'objet d'une déclaration de conformité en référence à la norme n° 46 (gestion des personnels des organismes publics et privés). Si un dispositif de contrôle individuel de la messagerie est mis en place, il doit être déclaré à la CNIL (déclaration normale), sauf désignation d'un correspondant informatique et libertés.

G. La diffusion de la charte informatique

Pour être opposable aux salariés la charte doit être déployée de la même manière qu'un règlement intérieur, à savoir :

-La diffuser individuellement.
-La diffuser collectivement, à une place accessible sur le lieu de travail.
-La soumettre au comité d'entreprise, ainsi qu'à l'avis du comité d'hygiène et de sécurité.
-La transmettre à l'inspection du travail.

En pratique, la charte doit être présentée à l'embauche d'un nouveau salarié, ce dernier doit en prendre connaissance et la signer au même titre que le règlement intérieur. Cette charte doit également être accessible à la collectivité pour consultation des droits de chacun. Elle peut pour cela être disponible sur l'intranet de l'entreprise ou tout simplement être affichée dans un lieu connu et accessible aux salariés.

III. FILTRAGE DE CONTENU

A. OBLIGATION D'INFORMATION

La mise en place d'une solution de filtrage constitue à la fois :

-Un outil de contrôle de l'activité des employés, et doit à ce titre être porté à leur connaissance.

-Une nouvelle technologie introduite au sein de l'entreprise, et doit en conséquence faire l'objet d'une consultation des institutions représentatives du personnel.

Dès lors que l'outil de filtrage engendre la collecte des données à caractère personnel, un document doit être rédigé pour informer les salariés individuellement et collectivement de la mise en place de cet outil. En outre l'entreprise se doit de faire une déclaration dite « normale » auprès de la CNIL.

L'explication simple du moyen et de la finalité d'une solution de filtrage de contenu sera insérée dans la charte informatique de l'entreprise ce qui favorisera à la fois sa diffusion et son opposabilité auprès des salariés.

B. ASPECTS JURIDIQUES

1. Aspect légal : le droit de filtrer

Il existe de nombreux textes de lois en rapport plus ou moins direct avec la notion de filtrage :
-**Loi HADOPI.**
-Le Code de la propriété intellectuelle.
-Loi relative à la concurrence et à la régulation du secteur des jeux d'argent et de hasard en ligne.
-Plusieurs directives européennes.

En définitive il existe une quasi obligation de recourir à une solution de filtrage de contenu et ce pour prévenir certains comportements, illégaux d'une part et pouvant porter atteinte au bien de l'entreprise d'autre part.

Il existe par ailleurs, une jurisprudence riche qui précise les possibilités de mise en place d'une solution de filtrage de contenu. Par exemple une telle solution a déjà été imposée à des entreprises sur des contenus en lien avec : la vente d'objets nazis, la diffusion de contenus racistes, de propos négationnistes, l'utilisation de jeux en ligne ou encore concernant l'accès à des sites d'hébergement de vidéos.

2. Bonnes pratiques et normes

Dans son Guide pratique pour les employeurs et les salariés, la Cnil considère que « s'il n'est pas possible d'interdire « de manière générale et absolue » l'utilisation d'Internet à des fins non professionnelles, en se référant notamment au contexte de développement des moyens de communication ainsi qu'au contexte jurisprudentiel actuel, rien n'empêche l'employeur de limiter notamment l'accès de ses employés à Internet ».
Selon la commission, « une telle limitation de l'accès à Internet ne constitue pas par principe une atteinte à la vie privée des employés et se justifie notamment parce que l'usage d'Internet est en général reconnu à condition qu'un tel usage soit, selon la commission : raisonnable, ne réduise pas la productivité, ni les « conditions d'accès professionnel au réseau » ».
D'un point de vue pratique, la Cnil reconnaît la possibilité de mettre en place des dispositifs de filtrage de sites non autorisés : sites à caractère pornographique, pédophile, révisionniste…
Selon la Commission, « l'employeur peut imposer certaines mesures dans l'utilisation des systèmes d'information, justifiées pour la sécurité de l'organisme, telles que : l'interdiction de télécharger des logiciels, de se connecter à des forums « Chat », ou d'accéder à une messagerie électronique personnelle, à condition d'en informer les salariés ».

3. Le Droit de loguer

Le système de logs permet de tracer les usages individuels et constitue le meilleur moyen pour prévenir d'éventuels abus. Toutefois, comme le recommande la CNIL, un certain nombre de précautions sont à prévoir comme :

-Prévoir un système de journalisation c'est-à-dire un enregistrement dans des «fichiers de logs» des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux doivent conserver les évènements sur une période à définir (la CNIL recommande de ne pas excéder 6 mois).

-Prévoir au minimum la journalisation des accès des utilisateurs incluant leur identifiant, la date et l'heure de leur connexion, ainsi que la date et l'heure de leur déconnexion.

-Dans certains cas, il peut être nécessaire de conserver également le détail des actions effectuées par l'utilisateur, telles que les données consultées par exemple.

4. Modalités de mise en œuvre

Toute entité qui met en œuvre un outil de filtrage doit procéder aux formalités préalables imposées par la CNIL notamment une déclaration dite « normale » car le dispositif permet un contrôle individuel et/ou touche aux données à caractère personnel.

Cette déclaration doit préciser :
-La finalité du traitement.
-Les données à caractère personnel traitées.
-La ou les catégories de personnes concernées.
-La durée de conservation des données.

-L'indication de la date à laquelle les représentants du personnel ont été informés de la mesure de filtrage.

5. Nécessité d'expliquer aux utilisateurs.

Non seulement les représentants du personnel, mais tous les utilisateurs doivent être informés de la mise en place de la solution de filtrage de contenu. Cette solution doit apparaitre explicitement sur la charte informatique. Celle-ci étant déployée en annexe du règlement intérieur, elle est opposable à tous les employés en cas de litige.

6. La prise en main à distance

L'outil de prise en main à distance des postes informatiques doit être utilisé à bon escient, l'administrateur qui y recourt doit s'assurer d'avoir l'accord de l'utilisateur et doit tracer les opérations de maintenance qu'il effectue.

C. ACCES AUX DIVERS CONTENUS

1. Accès aux réseaux sociaux

L'entreprise peut interdire l'accès aux réseaux sociaux toutefois cet accès peut avoir des objectifs professionnels de communication et donc l'administration de l'accès peut être planifiée en fonction des besoins.

L'accès peut également être laissé libre, le contrôle des excès devant être réalisé par l'administrateur en fonction de critères définis à l'avance et en accord avec les salariés.

2. Accès au web

Toute structure proposant un accès public au web (Exemple : hot spot WIFI) est soumise aux réglementations en vigueur pour les fournisseurs d'accès à internet (FAI) et donc peut voir sa responsabilité engagée du fait des accès illicites des tiers. Le filtrage des contenus et l'enregistrement de log revêt donc un caractère obligatoire.

D. CONSEQUENCES EN CAS D'ABSENCE DE SOLUTION DE FILTRAGE DE CONTENU

Art L 336-3 du Code de la propriété intellectuelle:

« La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise. »

En clair, l'abonné (c'est-à-dire l'employeur) est garant du bon usage de ses salariés et est responsable pour eux d'où la nécessité du filtrage.

1. Exemples de contenus pouvant engager la responsabilité de l'entreprise

- Contenus pédopornographiques.
- Sites de jeux en ligne illégaux.
- Protection des droits d'auteur.
- Sites à caractères raciste, révisionniste.

2. La question de la responsabilité

La responsabilité de l'employeur sera toujours recherchée en premier lieu pour savoir s'il y a eu négligence dans la mise en place d'un système préventif adéquat.

L'utilisateur engage toujours sa responsabilité individuelle s'il réalise un acte illégal.

L'administrateur peut voir sa responsabilité engagée en cas d'incompétence ou de négligence fautive dans la mise en place des systèmes de contrôle. L'administrateur ne doit en aucun cas exécuter de demandes venant de l'employeur qui seraient contraires au droit.

DEUXIEME PARTIE : Plan de sécurisation des données

I. ENJEUX ET NECESSITES

E. Evolutions

La sécurité des données est devenue un enjeu capital dans notre société où la croissance de l'utilisation des outils numériques et informatiques est exponentielle. Nos données, c'est-à-dire l'ensemble de nos connaissances, de nos savoir-faire, de nos contacts, tendent de plus en plus à être numérisées et à être conservées sur des supports relevant de technologies informatiques.

Auparavant les données restaient sur des supports physiques (tel que le papier) et leur sécurisation passait, par conséquent, par des moyens « physiques ». De nos jours, si des supports physiques sont toujours nécessaires, ceux-ci utilisent les technologies informatiques ce qui met en œuvre une partie dite «logique».

Cette évolution permet une sécurisation plus grande des données mais également, en cas de négligence ou d'incompétence des responsables de cette sécurisation, il peut s'en suivre une perte totale d'une grande quantité de données et ce, de façon définitive.

F. Responsabilité

La CNIL nous informe que : « Tout responsable de traitement informatique de données personnelles doit adopter des mesures de sécurité physiques (sécurité des locaux), logiques

(sécurité des systèmes d'information) et adaptées à la nature des données et aux risques présentés par le traitement. Le non-respect de l'obligation de sécurité est sanctionné de 5 ans d'emprisonnement et de 300 000 € d'amende. Art. 226-17 du code pénal. »

Les responsables des systèmes d'information ont donc l'obligation de prévoir une stratégie de sécurisation des données adaptée aux exigences de l'entreprise ou de la structure qu'ils ont en charge.

Cette stratégie comportera quatre points majeurs :

- Mesures immédiates de sauvegarde.
- Sécurisation physique des données.
- Sécurisation logique des données.
- Information aux utilisateurs des bonnes pratiques.

Nous allons détailler maintenant ces quatre points en fonction de nos choix en vue de l'appel d'offre de la société Autoconcept.

II. MESURES IMMEDIATES DE SAUVEGARDE

Lors du déploiement des solutions mises en place pour l'entreprise Autoconcept, les données à caractère professionnel, qu'elles soient sur les postes (dossier utilisateur, archive mail etc.) ou sur le serveur, seront copiées directement sur un disque dur externe USB d'1To. Ces données seront dupliquées sur un serveur de la société HOTH INFO puis conservées dans un coffre ignifugé et étanche qui sera positionné dans l'entreprise Autoconcept mais dans un emplacement différent de la salle serveur. Le code permettant d'ouvrir ce dernier ne sera connu que du directeur d'Autoconcept, du technicien en charge de l'administration du système informatique du site et du directeur de HOTH INFO.

Cette redondance permettra d'avoir les données conservées dans trois lieux et supports différents. Ainsi on assure l'accessibilité à ces données et leur récupération en cas de défaillance du réseau informatique ou de sinistre des locaux d'Autoconcept.

Ce système de conservation des données sera par la suite la base du système de sauvegarde qui sera appliqué aux données de l'entreprise Autoconcept. Le but étant d'avoir toujours cette triple redondance d'accès aux données.

III. SECURISATION PHYSIQUE DES DONNES

Afin d'éviter toute possibilité d'accès à des données sensibles par des individus n'y étant pas autorisés, on prévoira de sécuriser les locaux d'Autoconcept de façon adéquate.

La salle des serveurs pouvant être verrouillée on s'assurera qu'elle le soit chaque fois qu'un technicien la quitte après une intervention. A l'avenir on pourra solliciter Autoconcept pour installer un système de porte à fermeture et verrouillage automatique avec un accès par badge.
De même tous les bureaux doivent pouvoir être verrouillés pour éviter les tentatives d'intrusion.

Un système d'alarme anti-intrusion fonctionnel et vérifié périodiquement est également un élément indispensable pour la sécurisation physique d'accès aux données.

Enfin, pour s'assurer de la continuité d'activité, il conviendra d'avoir dans la salle serveur :
-Une climatisation avec un contrat de maintenance incluant une intervention immédiate lorsque la température détectée dans la salle dépasse un certain seuil.
-Un détecteur de fumée déclenchant une alarme en cas de départ de feu.
-Un onduleur capable de protéger les serveurs et autres périphériques réseaux des variations de tension, et, en cas de coupure totale de courant électrique d'assurer le maintien en activité des équipements pour une durée de 3 heures.

IV. SECURISATION LOGIQUE DES DONNEES

A. Stratégie logicielle

La stratégie de sauvegarde que nous proposons à l'entreprise Autoconcept consistera en la sauvegarde des données présentes sur le serveur de fichier selon le plan suivant :

-Une sauvegarde incrémentielle quotidienne durant la nuit.
-Une sauvegarde complète hebdomadaire le vendredi soir qui sera répliquée en mode synchrone (excellente fiabilité pour des courtes distances entre les sites) sur un serveur chez HOTH INFO.
-Une sauvegarde complète mensuelle sur le disque dur externe qui sera ensuite mis en sécurité dans le coffre ignifugé et étanche.

Les deux premiers points ci-dessus seront réalisés par le moyen d'un NAS (Network Attached Storage) qui est un boitier de stockage en réseau.

Pour éviter toute perte de données en cas de défaillance de ce matériel, celui-ci sera monté avec 2 disques durs d'1 To fonctionnant selon la technologie RAID 1(Redundant Array of Independent Disks). Cette technologie permet la redondance de la totalité des données sur chacun des disques durs et un accès plus rapide pour les utilisateurs. La défaillance d'un de ces disques n'engendre aucune conséquence. Tant qu'un des disques reste fonctionnel, l'intégrité des données est conservée. Il suffit de remplacer le ou les disques durs défaillants et le contrôleur RAID reconstitue le « Miroir» sur les nouveaux éléments.

B. Sécurisation des postes de travail

1. Authentification des utilisateurs

Au cours de la mise en place de la nouvelle architecture informatique chez Autoconcept, un domaine sera créée ce qui permettra un accès individualisé au ressources de l'entreprise, et d'autres part cela facilitera la gestion des droits d'habilitation des différents niveaux de sensibilité des données.

Conformément à ce que nous avons rédigé dans la charte informatique que nous proposons à l'entreprise Autoconcept, et suivant les recommandations de la CNIL :

-Chaque utilisateur se verra remettre un identifiant individuel d'accès à une session du domaine de l'entreprise et un mot de passe. La politique en matière de mot de passe au sein d'AUTOCONCEPT se résume en ceci :

- Changement du mot de passe lors de la première connexion.
- Le mot de passe doit comporter au minimum 8 caractères dont majuscule(s), minuscule(s) et chiffre(s) ou caractère(s) spécial (aux).
- Le mot de passe devra être changé tous les 3 mois et ne devra pas être identique à l'un des trois derniers mots de passe choisis.
- Le mot de passe ne doit jamais être communiqué à un tiers (Administrateur y compris)

Le technicien en poste sur site aura pour mission de veiller à la bonne application de cette procédure et d'aider individuellement chaque utilisateur dans sa première connexion.

- L'accès aux postes de travail et aux applications s'effectue à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2…), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants.

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

Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné.

-L'oubli d'un mot de passe fera l'objet d'une réinitialisation avec nécessité de le changer lors de première connexion, l'administrateur n'a donc jamais connaissance des mots de passe des utilisateurs.

-Un certain nombre de comportements sont à éviter, comme de ne pas configurer les logiciels pour qu'ils enregistrent les mots de passe, utiliser le même mot de passe pour différents accès (messagerie, ERP, session domaine…), stocker ses mots de passe sur des supports accessibles à tous (post-it, carnet sur le bureau…)

2. Gestion des habilitations

En concertation avec la direction d'Autoconcept, une stratégie en matière de droits d'accès aux ressources de l'entreprise sera définie. Chaque salarié se verra attribuer des droits en cohérence avec ses fonctions et son niveau hiérarchique. Les niveaux d'habilitation sont de trois types : lecture, écriture et modification.
Les droits d'accès pourront être révisés ponctuellement ou définitivement au gré des circonstances dans le sens de l'autorisation comme de la restriction.

3. Sécurité des postes

Afin de se prémunir des tentatives d'attaques venant de l'extérieur, qu'il s'agisse d'internet ou de tentative d'accès physique par des individus mal intentionnés, la connexion internet de l'entreprise sera soumise à un dispositif de pare-feu et un logiciel d'antivirus sera installé sur chaque poste.
Les mises à jour de ces logiciels ainsi que des systèmes d'exploitation utilisés seront effectués régulièrement par le technicien sur site afin de diminuer tout risque de menace.

La configuration des postes pour que la session de l'utilisateur se verrouille après un délai de 10 minutes et la recommandation faite de verrouiller celle-ci à chaque départ de son poste sont des mesures visant à prévenir l'accès à des donnés par des tiers ou bien par des salariés ne disposant pas du même niveau d'habilitation.

Pour ce qui concerne les ordinateurs portables, nous déciderons avec Autoconcept de la possibilité de crypter les données contenus sur le disque dur de ceux-ci en fonction de la sensibilité et du dommage que pourrait entrainer une perte de ces données. La clé de chiffrement serait dans ce cas connue uniquement de l'utilisateur, du directeur d'Autoconcept et du directeur de HOTH INFO.

V. DIFFUSION DES INFORMATIONS AUX UTILISATEURS

Les modalités de diffusion aux utilisateurs se feront par différents biais :

-L'approbation par les représentants du personnel et le comité d'entreprise de la charte informatique.

-La diffusion de la charte informatique comme annexe du règlement intérieur devant être signé par chaque membre de l'entreprise.

-L'affichage de cette même charte à un endroit connu afin de permettre sa consultation par les salariés.

-L'explication par le technicien de la finalité des moyens mis en place en vue d'une plus grande sécurité.

-L'accompagnement par le technicien pour la première connexion au domaine, à la messagerie, etc…

TROISIEME PARTIE : Charte Qualité Client Service

I. LA CHARTE QUALITE HOTH INFO

La charte sera également ajoutée en annexe dans sa version destinée à être diffusée, c'est-à-dire tenant sur une seule page.

CHARTE QUALITE

CONFIDENTIALITE

HOTH INFO fournit à ses clients un système informatique respectant les dispositions législatives, règlementaires et déontologiques. **La confidentialité des données du professionnel est assurée.**

COHERENCE

HOTH INFO s'assure de la compatibilité des différents éléments du système informatique et de leur bon fonctionnement d'ensemble. Nous analysons les problématiques de nos clients avec eux pour leur proposer les solutions les plus adaptées.

EVOLUTIVITE

HOTH INFO reste à l'écoute des besoins de ses clients et pratique une politique de veille technologique afin de comprendre l'évolution de son environnement pour proposer à ses clients les évolutions nécessaires à leur compétitivité.

SECURITE

En plus de mettre en place des stratégies visant à diminuer au maximum tout risque de perte de données ou autre dysfonctionnent informatique, HOTH INFO héberge en interne toutes les données sensibles de ses clients.

PROXIMITE

Nous travaillons en toute transparence avec nos clients c'est pourquoi il nous faut les connaitre. Nous proposons à chacun de nos clients des rencontres périodiques pour établir des bilans concernant notre prestation mais aussi pour comprendre leurs nouveaux besoins et leurs attentes à notre égard.

CONSEIL et FORMATION

Les compétences variées de HOTH INFO nous permettent de proposer des solutions adaptées et de former les utilisateurs finaux à ces technologies.

RAPIDITE

Chacun de nos contrats fait l'objet d'un accord concernant la résolution des incidents et les délais dans lesquels nous nous engageons à restaurer l'activité.

II. ENGAGEMENTS HOTH INFO ENVERS AUTOCONCEPT

A. Confidentialité

Dans le cadre de chaque nouveau partenariat, nos équipes en charge de l'étude de marché actualisent leurs connaissances en matière de législations informatiques ce qui garantit un respect total des lois en vigueur au sein de l'entreprise cliente : Autoconcept.

Les résultats de cette analyse sont présentés dans la première partie de ce document.

Dans le cadre du partenariat avec Autoconcept, toutes les informations la concernant elle ou son activité, seront traitées avec un soin particulier afin d'éviter tout risque de divulgation à des entreprises concurrentes.

B. Cohérence et Proximité

En outre de l'apport de solutions immédiates et prévisionnelles, nous nous engageons à réévaluer les besoins informatiques chez Autoconcept durant les trois premiers mois de prestation puis nous proposons à la société d'effectuer un bilan annuel et chaque fois que nos clients le jugeront nécessaire afin d'être totalement transparents sur notre activité.

Cette stratégie permettra une autoévaluation de notre partenariat, et de remédier à des imperfections qui pourraient avoir été signalées. Au cours de ces bilans périodiques, seront abordés des points tels que : l'attitude des techniciens, leur communication avec les salariés

d'Autoconcept, les bilans d'activité, les orientations d'avenir (investissement matériel, logiciel…).

C. Sécurité

Un plan de sauvegarde comprenant des mesures immédiates ainsi qu'une stratégie de sécurisation des données (politique de mot de passe, bonnes conduites à adopter…) vous sont présentés dans nos propositions.

Ces mesures assureront la pérennité de l'utilisation des données d'Autoconcept en cas de défaillance matériel ou d'incident quel qu'il soit. L'intégrité financière de la société en sera donc préservée.

D. Evolutivité

Nous proposons à la société Autoconcept, une actualisation de son parc informatique par un renouvellement de certains équipements. Si des évolutions nous semblent nécessaires par la suite nous proposerons à Autoconcept les solutions les plus adaptées.

E. Rapidité

Notre stratégie de gestion des incidents est présentée afin de donner à Autoconcept l'assurance d'une reprise de toute activité dans les trente minutes suivant une demande d'intervention.

Les détails de cette stratégie seront présentés plus tard dans cette partie.

F. Conseil et Formation

Nous proposons une formation des utilisateurs à chaque évolution de technologie et sur demande de nos clients. Chez Autoconcept nous souhaitons initier les utilisateurs au nouveau système d'exploitation (Windows Seven) qui va être déployé sur un certain nombre de postes ainsi qu'à la suite d'outils bureautiques associée (Microsoft Office 2013).

Nous proposons également, en supplément de notre prestation, des temps de formation à la demande pour répondre aux attentes de notre client (bureautique, messagerie, bonnes pratiques…).

III. Stratégie de continuité et Gestion d'incident

A. DISPONIBILITE DES PERSONNELS

Dans le cadre du partenariat avec la société Autoconcept, notre stratégie consistera à garder un technicien à plein temps sur site pour assurer les interventions à caractère urgent ainsi que les taches d'administration ne nécessitant pas de compétences de niveau ingénieur.

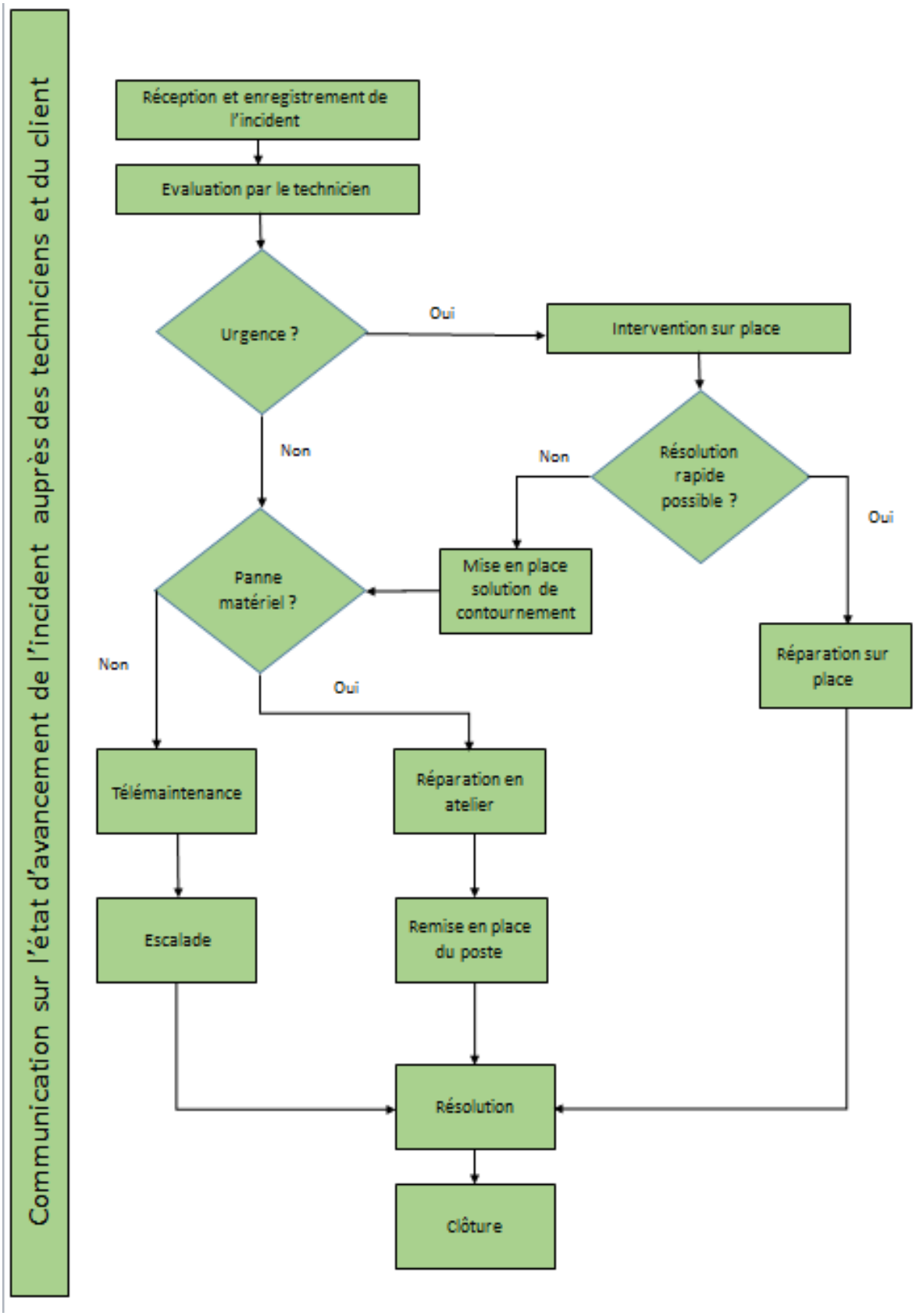
Nous aurons également un « niveau » technicien supplémentaire en infogérance depuis les locaux de HOTH INFO pour suppléer le technicien sur site en cas de besoin et qui sera

détaché sur site lors des périodes de congés du premier technicien ou en cas de besoin ponctuel de maintenance lourde.

Enfin nous mettrons à disposition les compétences de nos ingénieurs pour ajouter un niveau d'expertise en termes de gestion de parc et de résolution de problèmes.

B. GESTION DE LA CONTINUITE DE SERVICE

La contrainte imposée par la société Autoconcept consiste en l'obligation pour HOTH INFO de rétablir l'activité de tous les processus métiers en 30 minutes après la cessation de l'un d'eux.
HOTH INFO ne peut toutefois garantir un tel délai en cas de défaillance d'un opérateur externe à sa prestation : fournisseur d'accès internet, fournisseur d'énergie électrique, autre prestataire…

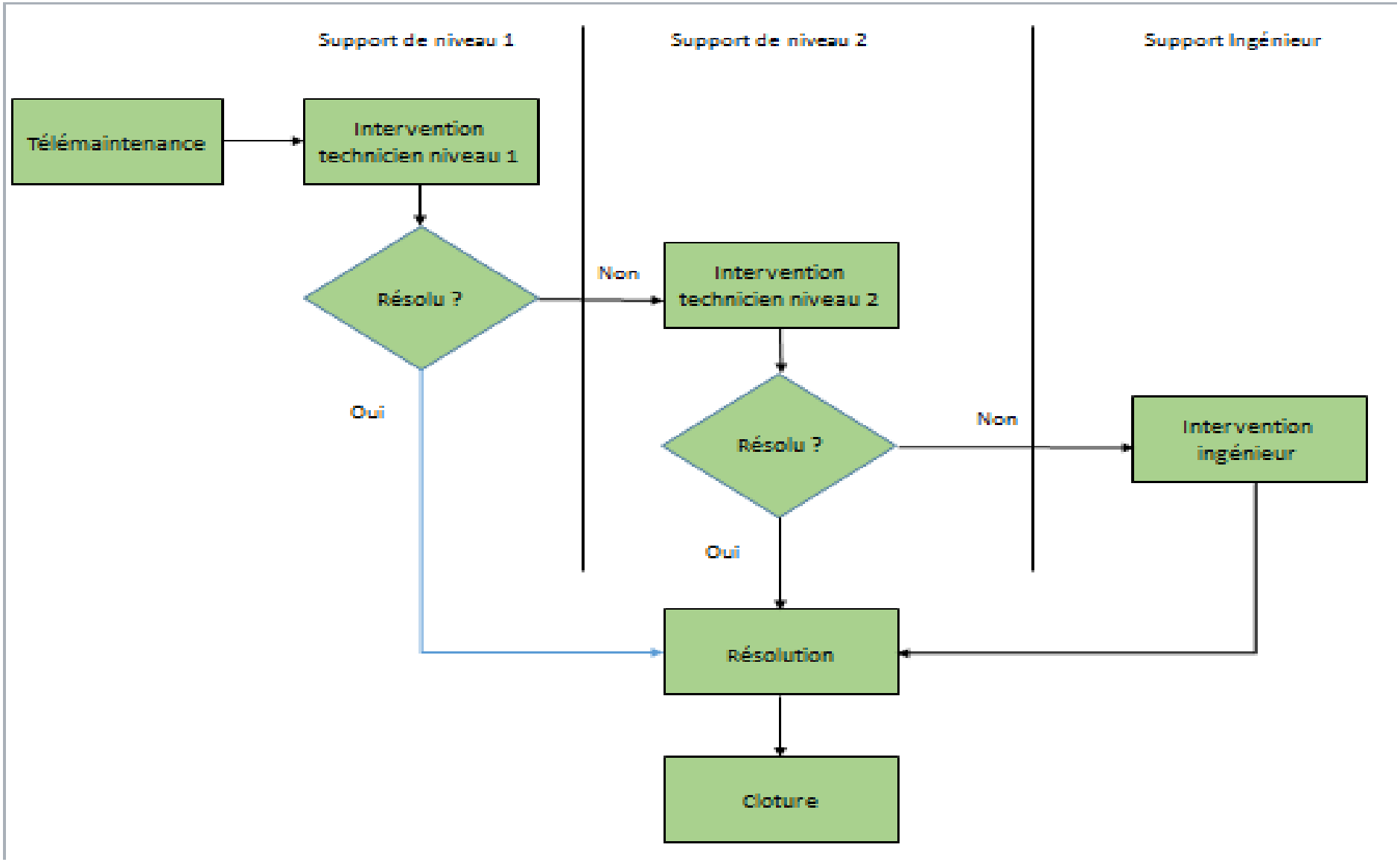

Communication sur l'état d'avancement de l'incident auprès des techniciens et du client
Réception et enregistrement de l'incident
Evaluation par le technicien
Urgence ?
Oui
Intervention sur place
Résolution rapide possible ?
Non
Oui
Non
Mise en place solution de contournement
Panne matériel ?
Réparation sur place
Non
Oui
Télémaintenance
Réparation en atelier
Escalade
Remise en place du poste
Résolution
Clôture

C. GESTION DES INCIENTS

Nous mettrons à disposition de tous les utilisateurs du système informatique de la société Autoconcept, une plateforme URL sur laquelle ils pourront créer un ticket d'incident pour signifier au service informatique : un incident, une demande, ou d'autres motifs à définir avec Autoconcept.

Recevrons les tickets : le technicien sur place et les techniciens en infogérance chez HOTH INFO(chacun pouvant évaluer s'il s'agit de son domaine de compétence). Chaque action concernant un ticket sera tracée sur la plateforme puis diffusée à l'utilisateur et aux techniciens par voie de courriel.
En cas d'escalade, le technicien le mentionne dans la fiche d'intervention ce qui génère un courriel à nos deux ingénieurs qui peuvent prendre connaissance du problème. Cette mesure leur permet d'anticiper sur un incident en cas d'escalade jusqu'à leur niveau.

Une fois résolu, le ticket est clôturé et l'ensemble des acteurs de cette résolution ainsi que l'utilisateur recevra une confirmation de clôture. L'utilisateur aura trois jours pour rouvrir le ticket en cas de persistance ou récurrence de l'incident via le champ prévu à cet effet dans le formulaire de clôture.


Support de niveau 1
Support de niveau 2
Support Ingénieur
Télémaintenance
Intervention technicien niveau 1
Résolu ?
Non
Intervention technicien niveau 2
Oui
Résolu ?
Non
Intervention ingénieur
Oui
Résolution
Cloture

D. GESTION DE FOND DE LA CONTINUITE DE SERVICE

Dans les trois premiers mois de prestation, HOTH INFO s'engage à réaliser une étude plus approfondie du parc informatique et de l'environnement de la société Autoconcept afin d'analyser tous les risques susceptibles de provoquer des cessations de processus métier et d'en rechercher des solutions préventives et curatives. L'élaboration de plans de reprise d'activité sera également réalisée en fonction des résultats des analyses préalables. Des tests seront effectués pendant des périodes sans activité (weekends, fermeture de l'entreprise) et des procédures rédigées afin de faciliter la mise en place en temps réel des solutions.

E. EVALUATION DU COUT DE PRESTATION

Dans le cadre de la signature éventuelle du contrat de prestation informatique avec la société Autoconcept, nous avons évalué les coûts, d'une part de la prestation et d'autre part du renouvellement impératif de matériel.

1. Renouvellement de matériel

Au vu de l'inventaire qui nous a été fourni par Autoconcept, il existe 46 postes fixes installés avec Windows XP ainsi que 4 ordinateurs portables.
Ces ordinateurs n'étant pas suffisamment performants pour supporter le système d'exploitation Windows 7, et Windows XP ne bénéficiant plus de support et de mises à jour de sécurité depuis mars 2014, la vulnérabilité de ces postes met en danger les données et la sécurité de l'entreprise. Il est donc impératif de les renouveler en tout premier lieu.

Nous pensons également qu'il est indispensable de se munir d'ordinateur de spare afin de pouvoir respecter notre engagement de continuité de service, à savoir reprise d'activité dans les 30 minutes. Nous avons un parc de 70 ordinateurs donc nous souhaitons au minimum 5 ordinateurs de spare ce qui fait un investissement à prévoir de 51 ordinateurs fixes et 4 ordinateurs portables.
Nous proposons des LENOVO H515S pour les postes fixes que notre partenaire nous vend à 228 euros l'unité et des LENOVO Thinkpad E540 à 370 euros l'unité pour les ordinateurs portables.

LENOVO H515S :
- Processeur AMD E1-2500 (1.40GHz 1333MHz 1MB).
- Carte/Chipset Graphique. Graphiques intégrés AMD.
-Mémoire vive : 4.0GB PC3-12800 DDR3 SDRAM 1600 MHz.
-Disque dur : 1TB 7200 rpm.
-Lecteur : Blu-ray/DVD-RW.
-Garantie : 1 an.
-Vendu sans système d'exploitation dans le cadre de notre partenariat avec LENOVO.

LENOVO Thinkpad E540 :
-Processeur Intel Core i3-4000M (non-vPro).
-Écran 15,6 pouces HD (1366 x 768) antireflets - Capot noir.
-Mémoire vive : 4 Go de mémoire DDR3L PC3-12800 (1 SODIMM).
- Disque dur 500 Go, 7200 tr/min.
-Graveur de DVD 8x, double couche.
-Carte WiFi Intel Wireless-N 7260 2X2 BGN + Bluetooth.
-Batterie lithium-ion 6 cellules 48 Wh, 75+.
-Garantie 1 an retour atelier.
-Vendu sans système d'exploitation dans le cadre de notre partenariat avec LENOVO.

Ces 55 ordinateurs devront être équipés d'un système d'exploitation Windows 7 professionnel, dont le prix unitaire de la licence(lot de 10) est de 95 euros.

Pour éviter tout problème de compatibilité entre versions des logiciels de la suite Microsoft Office, et pour anticiper sur les développements futurs dans ce domaine, nous proposons à Autoconcept d'équiper l'intégralité des 70 ordinateurs de la suite Microsoft Office 2013 : le coût étant de 12.30 euros par utilisateur et par an.

Le renouvellement des licences pour l'antivirus Nod 32 à 8.35 euros.

Le tableau ci-dessous récapitule ces divers éléments :

Coût du renouvellement de matériel

Matériel	Coût unitaire	Quantité	Totale
PC Fixe LENOVO H515S	228	51	11628
PC Portable LENOVO Thinkpad E540	370	4	1480
Licence Windows 7	95	55	5225
Microsoft Office 2013	12,3	70	861
Antivirus Nod 32	8,35	71	592,85
			19786,85
Marge sur matériel (10%)			
Coût de mise en place(10% du prix matériel)			
		Coût Total	**23744,22**
		Gain Hoth info: 4000euros	

Notons qu'il sera à prévoir également dans un futur proche, le renouvellement des systèmes d'impression dont l'ancienneté peut laisser penser que des défaillances se produiront et perturberont l'activité d'Autoconcept.
Egalement le serveur de fichier pourra être renouvelé afin d'avoir des niveaux harmonisés de matériel sur tout le parc informatique.

2. Cout de la prestation

Le forfait de la prestation que nous proposons à Autoconcept comprend :

- Un technicien de maintenance à temps plein sur site pour assurer tout le support de niveau 1, permettre le respect de la reprise d'activité en 30 minutes en cas d'incident et le maintien en état fonctionnel de l'architecture informatique qui sera mise en place. Nous nous basons sur une marge de 25% par rapport au coût de revient de ce même technicien pour HOTH INFO.
- Un forfait technicien de 50h par mois (soit 15h par semaine). Ce forfait intègre 15h/mois correspondant au remplacement du premier technicien pendant ces congés payés ainsi que le prévisionnel de diverses prestations qui devront être réalisées par un des techniciens de HOTH INFO en fonction des compétences requises. Le prix horaire étant de 65 euros.
- Un forfait Ingénieur de 20h par mois correspondant à un prévisionnel des interventions qui devront être réalisées par nos deux ingénieurs en termes de réseau ou de système. Le prix horaire étant de 115 euros

Tableau récapitulatif :

Coût de la prestation

Prestation	Coût horaire	Quantité	Totale
Technicien supérieur sur site	21,375	151,67	3241,94625
Technicien supérieur à distance	65	50	3250
Ingénieur Système	115	10	1150
Ingénieur Réseau	115	10	1150
			8791,94625

Le coût mensuel de la prestation demandé à Autoconcept sera donc de 8800 euros.

QUATRIEME PARTIE : Mémo Interne

Une note de service à l'intention de tous les salariés de HOTHINFO, afin de redéfinir les attentes de la direction, en ce qui concerne l'attitude à avoir dans l'exercice de ses fonctions au cours d'une prestation dans une entreprise cliente.
Cette note de service est présentée en annexe et elle est accompagnée d'un schéma récapitulatif des bonnes pratiques d'un technicien informatique et d'un autre concernant la bonne gestion d'un appel téléphonique.

CONCLUSION

Cette étude dans le cadre de l'appel d'offre de la société Autoconcept permet de proposer à celle-ci une solution sécurisante juridiquement car les connaissances en ce domaine ont été actualisées chez HOTH INFO ; mais également en terme sécurité et de productivité.

Une solution avec un coût abordable qui permet le maintien d'une continuité d'activité, et ce, en étant transparent sur les moyens et les méthodes.

La stratégie de sécurisation des données assure différents niveaux de sécurité avec une relative facilité de mise en place.

Les engagements qualité et le plan de continuité sont exposés clairement afin de rassurer notre futur client qu'il s'agisse de l'attitude de nos techniciens et ingénieurs ou du plan d'action en cas d'incident.

Enfin notre politique visant à effectuer des bilans périodiques de notre activité garantie une adaptabilité de notre entreprise aux besoins changeant de notre futur client.

SOURCES ET REFERENCES BIBLIOGRAPHIQUES

Législations :

http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460
http://travail-emploi.gouv.fr/informations-pratiques,89/les-fiches-pratiques-du-droit-du,91/sanctions-et-pouvoir-disciplinaire,111/le-reglement-interieur,1010.html

http://www.legifrance.gouv.fr/affichCode.do?idArticle=LEGIARTI000006417945&idSectionTA=LEGISCTA000006181756&cidTexte=LEGITEXT000006070719&dateTexte=20140530

CNIL :

www.cnil.fr

http://www.cnil.fr/linstitution/missions/

http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/

Guide pour employeurs et employés :
http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL_GuideTravail.pdf

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_securite-VD.pdf

http://www.cnil.fr/les-themes/securite/fiche-pratique/article/10-conseils-pour-securiser-votre-systeme-dinformation-1/

http://www.cnil.fr/fileadmin/documents/approfondir/dossier/travail/FICHETRAVAIL_INFORMATIQUE.pdf

http://www.cnil.fr/les-thames/travail/fiche-pratique/article/lacces-a-la-messagerie-dun-salarie-en-son-absence

http://www.cnil.fr/linstitution/actualite/article/article/le-controle-de-lutilisation-dinternet-et-de-la-messagerie/

http://www.cnil.fr/linstitution/actualite/article/article/lutilisation-par-les-organisations-syndicales-de-lintranet-et-de-la-messagerie-electronique-d/

http://www.cnil.fr/les-themes/identite-numerique/fiche-pratique/accessible/non/article/lutilisation-de-limage-des-personnes/

Charte Informatique :

http://www.yakakliker.org/@api/deki/files/623/=guide-charte-informatique-olfeo.pdf

Charte informatique du Groupe CESI de 2012

Charte informatique du Comité technique paritaire de 2010

cnil_fiche_n25_clause de confidentialité

www.toulouse.cci.fr/.../download.asp?.../Elaborer...charte_informatique...

Livre blanc juridique Olfeo : http://www.olfeo.com/proteger-votre-entreprise/maitriser-le-cadre-juridique/plan-de-deploiement-dune-solution-de-filtrage

ITIL :

http://www.itilfrance.com/

Gestion des incidents :
http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/10-2-index_inc.inc&pg=menu_itilv2.inc&ps=sousmenu_itil.inc&pt=La%20gestion%20des%20incidents&pb=haut_entete_itilv2.inc

Gestion de la continuité de service :
http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/21-5-index_cont.inc&pg=menu_itilv2.inc&ps=sousmenu_itil.inc&pt=La%20gestion%20de%20la%20continuit%E9%20de%20service&pb=haut_entete_itilv2.inc

Gestion de la disponibilité :
http://www.itilfrance.com/index.php?pc=pages/docs/itilv2/21-5-index_cont.inc&pg=menu_itilv2.inc&ps=sousmenu_itil.inc&pt=La%20gestion%20de%20la%20continuit%E9%20de%20service&pb=haut_entete_itilv2.inc

Charte Qualité :

http://www.sinequanon.fr/public/notre_charte/seo/charte-qualite-maintenance-informatique-reactivite

http://www.epsilog.com/epsilog/notre-charte-qualite.html

http://idos.fr/index.php?action=charte

http://www.commentcamarche.net/contents/999-mise-en-place-d-une-demarche-qualite

http://www.commentcamarche.net/contents/1008-qualite

http://www.entreprises.gouv.fr/politique-et-enjeux/qualite/notions-cles

LISTE DES ANNEXES

ANNEXE 1 :
Charte informatique proposée à Autoconcept

ANNEXE 2 :
Mémo Interne : NOTE DE SERVICE N°328 05/14

ANNEXE 3 :
Mindmap sur la gestion des appels téléphoniques

ANNEXE 4 :
Charte Qualité HOTH INFO 1 page

ANNEXE 5 :

Mindmap sur le comportement d'un technicien de maintenance informatique

ANNEXE 6 :

Estimation de la masse salariale de HOTH INFO et du montant de ses frais généraux ayant servi au calcul du coût de la prestation

ANNEXE 7 :

Formulaire de création de ticket.

ANNEXE 8 :

Formulaire de demande d'intervention.

CHARTE INFORMATIQUE

AUTOCONCEPT

Contenu

I. PREAMBULE

La charte informatique a pour but d'expliciter les modalités d'utilisation des systèmes d'information disponibles au sein de la société AUTOCONCEPT. Le développement exponentiel de ces systèmes, notamment informatiques oblige à définir un certain nombre de règles d'usage à l'intention des utilisateurs et des administrateurs de ces outils. Ceux-ci visant à garantir la sécurité de l'entreprise et de ses collaborateurs, à préciser leur responsabilité devant les législations en vigueur et enfin à assurer une transparence totale

sur la politique de l'entreprise en ce qui concerne la gestion des données et leur utilisation. En effet, une mauvaise utilisation de ces outils peut avoir des conséquences extrêmement graves : risques d'atteinte à la confidentialité, de mise en jeu de la responsabilité personnelle ou de l'entreprise, d'atteinte à l'intégrité et à la sécurité des fichiers de données personnelles (virus, intrusions sur le réseau interne, vols de données).De plus, mal utilisés, les outils informatiques peuvent aussi être une source de perte de productivité et de coûts additionnels.

II. DEFINITIONS

On rassemblera de façon générale sous le terme "ressources informatiques", les moyens informatiques de calcul ou de gestion locaux ainsi que ceux auxquels il est possible d'accéder à distance, directement ou en cascade à partir du réseau administré par l'entreprise.

On désignera par "services internet", la mise à disposition par des serveurs, locaux ou distants, de moyens d'échanges et d'informations diverses (web, messagerie, forum, réseaux sociaux, « microblogging », etc...).

On désignera sous le terme "utilisateur", les personnes ayant accès ou utilisant les ressources informatiques et services internet.

Parallèlement, le terme « administrateur » désignera les personnes en charge du maintien de l'intégrité du système d'information. Sont à leur charge : la mise en place, la maintenance, le développement du système d'information. Et pour ce faire ils disposent de tous les moyens évoqués dans la charte informatique.

III. PORTEE ET OPPOSABILITE

A. Les personnes concernées par la charte informatique

La présente charte s'applique indistinctement à toutes les catégories citées ci-dessous :

- Les utilisateurs internes à l'entreprise n'exerçant aucune fonction d'administration des systèmes d'information quel que soit leur niveau hiérarchique dans l'entreprise.

- Les administrateurs des systèmes d'information.

- Tous les collaborateurs externes exerçant une action ponctuelle au sein de la structure. S'il s'agit d'entreprises tierces, les contrats souscrits entre et celles-ci et AUTOCONCEPT et donnant accès aux données, aux programmes informatiques ou à tout autre moyen d'AUTOCONCEPT devront stipuler que ces utilisateurs s'engagent à respecter la présente charte.

- L'ensemble des intervenants de la société prestataire de service en charge de la gestion et de l'administration des systèmes informatiques à savoir « NOM DE L'ENTREPRISE ».

B. Les outils concernés par la charte informatique

Sont concernés par la présente charte, et par conséquent leurs utilisateurs se soumettent aux règles de bon usage indiquées dans celle-ci :

- Les postes informatiques fixes fournis par l'entreprise.
- Les ordinateurs portables à usage professionnel.
- Les téléphones portables et fixes à usage professionnel.
- Tout matériel de l'entreprise pouvant être connecté au réseau de l'entreprise (photocopieurs, imprimantes, scanners…)
- Les logiciels installés sur les postes informatiques sont soumis aux droits d'auteur et à la propriété intellectuelle.
- L'intranet de l'entreprise.
- Tout média personnel (ordinateurs portables, téléphone portables…) ayant reçu une autorisation d'utilisation au préalable.
- Tout équipement informatique ou plus généralement numérique appartenant à un collaborateur externe ou à une société prestataire de service ayant accès au réseau interne de l'entreprise.

C. Politique de sécurité en matière de connexion au réseau de l'entreprise

La politique de l'entreprise en matière de connexion au réseau sera précisée dans les différents articles de la présente charte, toutefois les axes fondamentaux de celle-ci sont :

- L'accès individuel via un compte personnel.
- La sécurité des identifiants et des mots de passe utilisateur
- Le contrôle de l'accès au Web dans le respect des libertés individuelles conformément à la législation en vigueur.
- L'enregistrement de logs et leur conservation sur une durée de 6 mois.

D. Opposabilité de la Charte

La présente charte, ayant été étudiée et validée par les représentants du personnel ainsi que par le comité d'entreprise a été annexée au règlement intérieur de l'entreprise et a fait l'objet d'une validation auprès de l'inspection du travail. La stratégie de filtrage de contenu a fait l'objet d'une déclaration simple auprès de la CNIL.
Elle est consultable à tout moment sur le réseau interne de l'entreprise ou auprès des représentants du personnel.

IV. Définition des conditions d'accès et d'identification

La loi "informatique et libertés" impose que les organismes mettant en œuvre des fichiers garantissent la sécurité des données qui y sont traitées. Cette exigence se traduit par un ensemble de mesures que les détenteurs de fichiers doivent mettre en œuvre, essentiellement par l'intermédiaire de leur direction des systèmes d'information (DSI) ou de leur responsable informatique.

A. Postes de travail et comptes utilisateur

Conformément aux recommandations de la CNIL en matière de sécurité des systèmes d'information :

-Chaque utilisateur se verra remettre un identifiant individuel et un mot de passe. La politique en matière de mot de passe au sein d'AUTOCONCEPT se résume en ceci :

- Changement du mot de passe lors de la première connexion.
- Le mot de passe doit comporter au minimum 8 caractères dont majuscule(s), minuscule(s) et chiffre(s) ou caractère(s) spécial(aux).
- Le mot de passe devra être changé tous les 3 mois et ne devra pas être identique à l'un des trois derniers mots de passe choisis.
- Le mot de passe ne doit jamais être communiqué à un tiers (Administrateur y compris)

- L'accès aux postes de travail et aux applications s'effectue à l'aide de comptes utilisateurs nominatifs, et non « génériques » (compta1, compta2…), afin de pouvoir éventuellement être capables de tracer les actions faites sur un fichier et, ainsi, de responsabiliser l'ensemble des intervenants.

- Les postes des agents sont paramétrés afin qu'ils se verrouillent automatiquement au-delà d'une période d'inactivité de 10 minutes ; les utilisateurs doivent également verrouiller systématiquement leur poste dès qu'ils s'absentent de leur bureau. Ces dispositions sont de nature à restreindre les risques d'une utilisation frauduleuse d'une application en cas d'absence momentanée de l'agent du poste concerné.

-L'oubli d'un mot de passe fera l'objet d'une réinitialisation avec nécessité de le changer lors de première connexion, l'administrateur n'a donc jamais connaissance des mots de passe des utilisateurs.

B. Conditions d'accès aux données

1. Utilisateurs Internes

L'accès aux données personnelles traitées dans un fichier est limité aux seules personnes qui peuvent légitimement y avoir accès pour l'exécution des missions qui leur sont confiées. Chaque agent se voit donc attribuer un « le profil d'habilitation » d'accès aux données en fonction des missions qui lui incombent. Pour chaque mouvement ou nouvelle affectation d'un salarié à un poste, le supérieur hiérarchique concerné doit identifier le ou les fichiers auxquels celui-ci a besoin d'accéder et faire procéder à la mise à jour de ses droits d'accès.

2. Prestataires de service

Conformément à l'article 34 de la loi « Informatique et Libertés » modifiée, une clause de confidentialité a été établie entre AUTOCONCEPT et l'entreprise XXXXXX. Le contrat nous liant à cette entreprise comprend ladite clause, celle-ci stipule que :

« Les supports informatiques et documents fournis par la société AUTOCONCEPT à la société XXXXX restent la propriété de la société AUTOCONCEPT.

Les données contenues dans ces supports et documents sont strictement couvertes par le secret professionnel (article 226-13 du code pénal), il en va de même pour toutes les données dont XXXXX prend connaissance à l'occasion de l'exécution du présent contrat.

Conformément à l'article 34 de la loi « Informatique et Libertés » modifiée, XXXXX s'engage à prendre toutes précautions utiles afin de préserver la sécurité des informations et notamment d'empêcher qu'elles ne soient déformées, endommagées ou communiquées à des personnes non autorisées.

XXXXX s'engage donc à respecter les obligations suivantes et à les faire respecter par son personnel :

– ne prendre aucune copie des documents et supports d'informations qui lui sont confiés, à l'exception des copies nécessaires à l'exécution de la présente prestation prévue au contrat. L'accord préalable du maître du fichier étant nécessaire ;

– ne pas utiliser les documents et informations traités à des fins autres que celles spécifiées au présent contrat ;

– ne pas divulguer ces documents ou informations à d'autres personnes, qu'il s'agisse de personnes privées ou publiques, physiques ou morales ;

– prendre toutes mesures permettant d'éviter toute utilisation détournée ou frauduleuse des fichiers informatiques en cours d'exécution du contrat ;

– prendre toutes mesures de sécurité, notamment matérielles, pour assurer la conservation et l'intégrité des documents et informations traités pendant la durée du présent contrat ;

– ne restituer les informations que sous forme agrégée afin de préserver l'anonymat des personnes ;

– à l'issue du contrat, procéder à la destruction de tous fichiers manuels ou informatisés stockant les informations saisies.

À ce titre, XXXXX ne pourra sous-traiter l'exécution des prestations à une autre société, ni procéder à une cession de marché sans l'accord préalable de AUTOCONCEPT.

AUTOCONCEPT se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées par XXXXX.

En cas de non-respect des dispositions précitées, la responsabilité du titulaire peut également être engagée sur la base des dispositions de l'article 226-17 du code pénal.

AUTOCONCEPT pourra prononcer la résiliation immédiate du contrat, sans indemnité en faveur du titulaire, en cas de violation du secret professionnel ou de non-respect des dispositions précitées. »

V. LE PRINCIPE DE PROPRIETE INTELLECTUELLE

A. Les Logiciels

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit. La copie d'un logiciel constitue le délit de contrefaçon.

L'utilisateur ne doit pas porter atteinte à la propriété intellectuelle d'autrui, notamment via la reproduction, la représentation ou la diffusion d'une œuvre en violation des droits de l'auteur ou de toute autre personne titulaire de ces droits.

En outre, dans les documents qu'il met à la disposition des tiers, l'utilisateur s'engage à respecter les droits d'auteur et ceux liés à la propriété intellectuelle. L'utilisateur ne doit pas lire, modifier, copier ou détruire d'autres fichiers que ceux qui lui appartiennent en propre, directement ou indirectement.

B. Le téléchargement

Conformément à la législation, tout téléchargement de contenu soumis aux droits d'auteur est interdit et fait l'objet d'une politique particulière visant à protéger l'entreprise de ce genre de comportement. Si toutefois, il est établi qu'un utilisateur a contourné les moyens mis en place à cet effet, ce dernier encourt une sanction (cf RESPONSABILITE ET SANCTION).

Le téléchargement de document destiné à l'usage professionnel, comme des fichiers .pdf par exemple, est autorisé dans la mesure où ces documents sont mis à la disposition du public par leur auteur.

VI. PROTECTION DES DONNEES A CARACTERE PERSONNEL

La Commission Nationale pour l'Informatique et les libertés (CNIL) stipule qu' « une utilisation personnelle de ces outils est tolérée par les tribunaux si elle reste raisonnable et n'affecte pas la sécurité des réseaux ou la productivité. C'est à l'employeur de fixer les contours de cette tolérance et d'en informer ses employés ».

De plus, elle précise : L'employeur peut contrôler et limiter l'utilisation d'internet (dispositifs de filtrage de sites, détection de virus…) et de la messagerie (outils de mesure de la

fréquence des envois et/ou de la taille des messages, filtres « anti-spam »...). Ce contrôle a pour objectif :
1. D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de Troie...).
2. De limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux…).

A. Les boites aux lettres électroniques

Par défaut, les courriels ont un caractère professionnel. L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.

L'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, cela constitue un comportement excessif.

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées. Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles. Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :
- en précisant dans leur objet « Personnel » ou « Privé »
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.

Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages. En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé.

L'utilisateur signera tout courriel professionnel. Elle comportera obligatoirement :
- Le nom et prénom de l'expéditeur
- La fonction de l'expéditeur
- Le service de rattachement
- Les coordonnées postales de l'entreprise.

En cas d'absence prévisible, l'utilisateur devra mettre en place un message automatique d'absence indiquant la date de retour prévue. Un agent du service doit pouvoir gérer les messages pendant son absence.

B. Les fichiers personnels

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement. Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder:
- en présence de l'employé ou après l'avoir appelé.
- en cas de risque ou évènement particulier, qu'il appartient aux juridictions d'apprécier.

Les administrateurs des ressources informatiques ont le devoir d'assurer un bon fonctionnement des réseaux et des ressources informatiques. Ils ont le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle. En particulier, les administrateurs des systèmes peuvent être amenés à examiner le contenu de fichiers ou boîtes aux lettres, et ce afin d'obtenir suffisamment d'informations pour pallier les incidents de fonctionnement ou dans le but de pouvoir déterminer si un utilisateur ne respecte pas la politique d'utilisation des ressources informatiques décrite dans la présente charte.

'L'article 38 de la loi « Informatique et Libertés » précise toutefois que « Toute personne physique a le droit de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement.
Elle a le droit de s'opposer, sans frais, à ce que les données la concernant soient utilisées à des fins de prospection, notamment commerciale, par le responsable actuel du traitement ou celui d'un traitement ultérieur ».

C. Mobilité, Absences, Départ

L'article 34 de la loi « Informatique et Libertés » explique que « le responsable du traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès ».

Ainsi en cas, de départ ou d'absence d'un utilisateur, toutes les données présentes sur son poste informatique sont susceptibles d'être récupérées, lues voire utilisées si celles-ci présentent un intérêt pour l'entreprise.

Toutefois il est souhaitable que chaque utilisateur amené à quitter ses fonctions de façon temporaire ou définitive ne laisse sur son poste informatique que des données en lien avec son activité professionnelle.

En cas de vol d'un équipement informatique professionnel (ordinateur portable, téléphone portable…), l'utilisateur est dans l'obligation de le signaler au plus vite à l'administrateur réseau. Ce dernier, en concertation avec la direction, prendra toute les mesures nécessaires à cet égard (dépôt de plainte, blocage des accès au réseau…)

VII. POLITIQUE DE TRACABILITE ET DE FILTRAGE DE L'ACCES A INTERNET

Un accès internet est accessible via un login utilisateur. Les utilisateurs se doivent d'en faire une utilisation liée à leur besoin professionnel et en respectant la présente charte.

Pour assurer la sécurité des équipements connectés et des utilisateurs, il existe un système de firewall et de filtrage d'accès internet sans pour autant porter atteinte à la vie privée de qui que ce soit.

L'accès internet est sécurisé et surveillé par :

- Un dispositif de filtrage des sites non autorisés : pornographie, pédophilie, haine raciale, apologie de tout type de crime et délit, contenu et téléchargement illégaux, etc. ;
- Un système de surveillance qui limite ou interdit de télécharger du contenu ou des logiciels ne respectant pas les besoins professionnels.

Chaque connexion sera enregistrée et le log sera conservé pour une durée de 6 mois.

L'accès à internet est donc contrôlé à des fins de sécurité tant pour les salariés que pour l'entreprise. En effet, Autoconcept fournissant un accès internet à ces usagers, elle se voit imposer les mêmes législations qu'un fournisseur d'accès à internet.

VIII. POLITIQUE DE CONSERVATION DES DONNEES

Une stratégie de sauvegarde des données a été établie en discussion avec notre prestataire de services informatiques HOTH INFO. Celle-ci consistant en une sauvegarde quotidienne des données présentes sur le serveur de fichier de l'entreprise.

En conséquence, il est fondamental que toute donnée soit sauvegardée par les utilisateurs sur ce même serveur. La préservation et la sécurisation de ces données, et de ces données seulement, est une mission prioritaire de notre prestataire.

HOTH INFO ne pourra aucunement être tenu responsable d'une perte de données si celles-ci se trouvaient sur le disque dur du poste ayant subi une défaillance ou un sinistre.

IX. RESPONSABILITE ET SANCTIONS

La loi, les textes réglementaires et la présente charte définissent les droits et obligations des personnes utilisant les ressources informatiques.

Tout utilisateur du système d'information de la collectivité n'ayant pas respecté la loi pourra être poursuivi pénalement.

En outre, tout utilisateur ne respectant pas les règles définies dans cette charte est passible de mesures qui peuvent être internes à l'établissement et/ou de sanctions disciplinaires proportionnelles à la gravité des manquements constatés par l'autorité territoriale.

X. DEROGATIONS

Des dérogations en ce qui concerne l'utilisation des ressources informatiques peuvent être accordées à des employés nécessitant un accès particulier dans le cadre de leur activité professionnelle. Ces dérogations doivent faire l'objet d'une demande préalable, laissant un délai suffisant pour la mise en place, et doivent être acceptées par la direction en concertation avec le responsable du système d'information.

XI. ENTREE EN VIGUEUR DE LA CHARTE

La présente charte, a été approuvée par les représentants du personnel, le comité d'entreprise, a été validée par l'inspection du travail. Son entrée en vigueur prend effet le 1er Juillet 2014.

Etant annexée au règlement intérieur elle s'impose à tous les membres de l'entreprise ainsi qu'à toute personne embauchée ultérieurement par Autoconcept.

Je soussigné (nom et prénom) ……..,

Déclare avoir pris connaissance des termes de la présente charte et m'engage à la respecter.

Fait le …….. à ……,

Signature (lu et approuvé à indiquer en mention manuscrite)

GUILLAUME HARDY
GEFFIER PIERRE-EMMANUEL

Dossier suivi par : Directeur

Objet : Conduite à tenir
au sein des entreprises clientes

Date : 25 Mai 2014

A L'INTENTION DE TOUS LES PERSONNELS

NOTE DE SERVICE N°328 05/14

Dans le cadre des contrats nous liant à nos clients il est rappelé à tous les personnels missionnés, ou bien intervenants sur site chez l'un d'eux, qu'une tenue vestimentaire correcte est indispensable, elle doit être en harmonie avec la norme imposée dans l'entreprise d'accueil. De plus, une ponctualité rigoureuse doit être respectée, ainsi qu'une attitude respectueuse et compréhensive à l'égard des salariés de nos entreprises clientes.

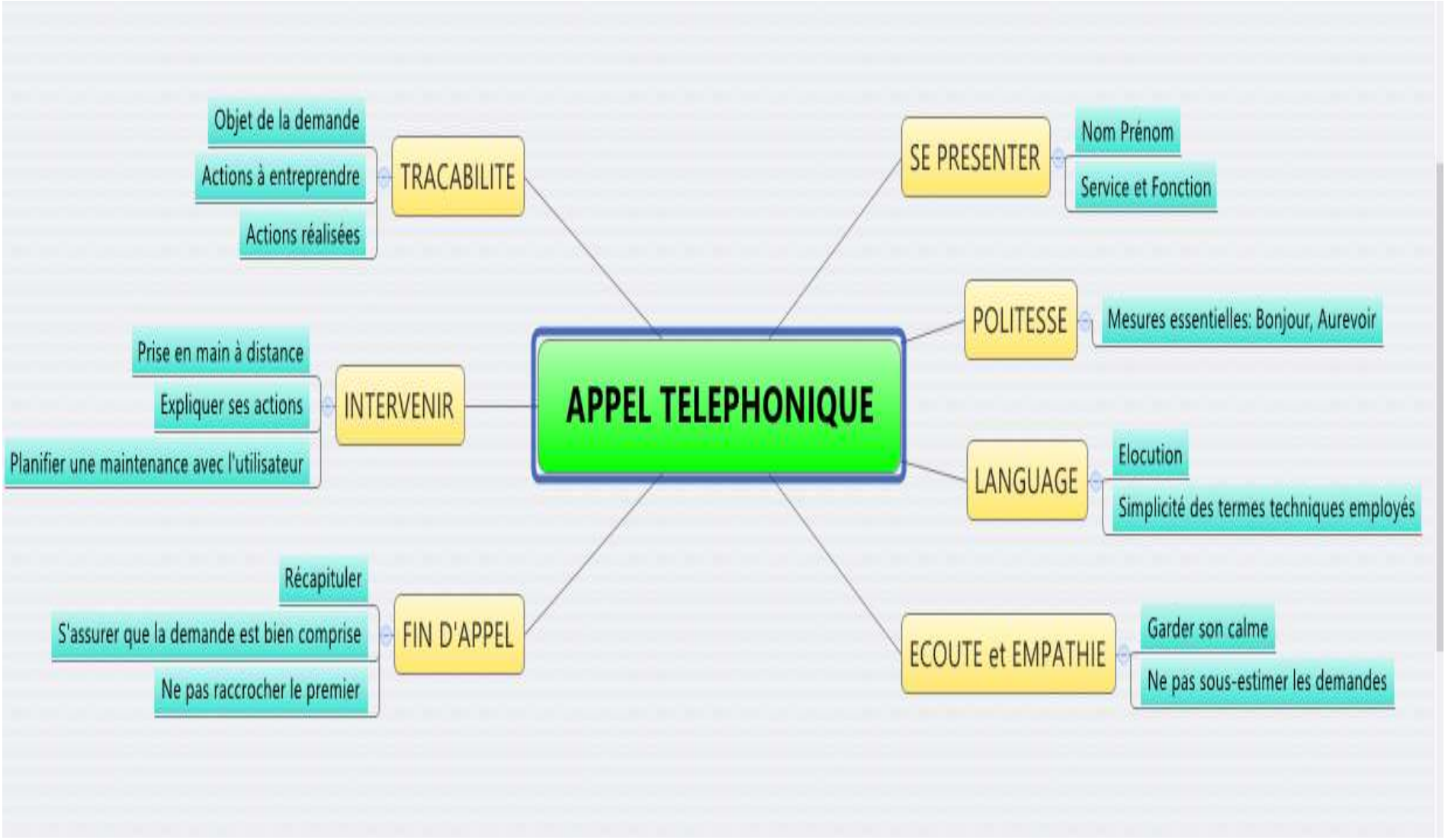
La satisfaction de nos clients passe d'une part par l'écoute et l'analyse des problématiques rencontrées, par une explication calme et adaptée du problème à l'utilisateur et d'une estimation réaliste du temps prévu pour la résolution. D'autre part la tenue des délais estimés de résolution reste une de nos priorités.

Il est indispensable d'établir l'ordre des tâches à réaliser en fonction de deux critères principaux : le degré d'urgence de l'intervention (un problème impliquant une cessation d'activité le rend prioritaire du fait l'obligation de continuité de service sur laquelle nous nous engageons), et la facilité de résolution de l'incident (le traitement un incident mineur mais de résolution simple ne doit pas être différé plus de quelques jours).

La gestion des réparations effectuées en atelier doit être transparente vis-à-vis des utilisateurs. Un appareil en réparation doit toujours faire l'objet d'un remplacement temporaire, les actes de maintenance envisagés doivent être expliqués à l'utilisateur et le temps d'indisponibilité de celui-ci évalué. Une fois la maintenance réalisée, il doit être restitué à l'utilisateur. Si le matériel est jugé défectueux, un nouveau matériel, au minimum équivalent sera proposé à l'utilisateur.

Enfin, il convient de respecter exactement les directives émanant des directions de nos entreprises clientes. Le contournement de celles-ci constitue une faute grave, excepté si elles viennent contredire le droit ou la charte informatique validée par la structure d'accueil.

La Direction


APPEL TELEPHONIQUE
TRACABILITE
Objet de la demande
Actions à entreprendre
Actions réalisées
SE PRESENTER
Nom Prénom
Service et Fonction
POLITESSE
Mesures essentielles: Bonjour, Aurevoir
INTERVENIR
Prise en main à distance
Expliquer ses actions
Planifier une maintenance avec l'utilisateur
LANGUAGE
Elocution
Simplicité des termes techniques employés
FIN D'APPEL
Récapituler
S'assurer que la demande est bien comprise
Ne pas raccrocher le premier
ECOUTE et EMPATHIE
Garder son calme
Ne pas sous-estimer les demandes

CHARTE QUALITE

CONFIDENTIALITE

HOTH INFO fournit à ses clients un système informatique respectant les dispositions législatives, règlementaires et déontologiques. **La confidentialité des données du professionnel est assurée.**

COHERENCE

HOTH INFO s'assure de la compatibilité des différents éléments du système informatique et de leur bon fonctionnement d'ensemble. Nous analysons les problématiques de nos clients avec eux pour leur proposer les solutions les plus adaptées.

EVOLUTIVITE

HOTH INFO reste à l'écoute des besoins de ses clients et pratique une politique de veille technologique afin de comprendre l'évolution de son environnement pour proposer à ses clients les évolutions nécessaires à leur compétitivité.

SECURITE

En plus de mettre en place des stratégies visant à diminuer au maximum tout risque de perte de données ou autre dysfonctionnent informatique, HOTH INFO héberge en interne toutes les données sensibles de ses clients.

PROXIMITE

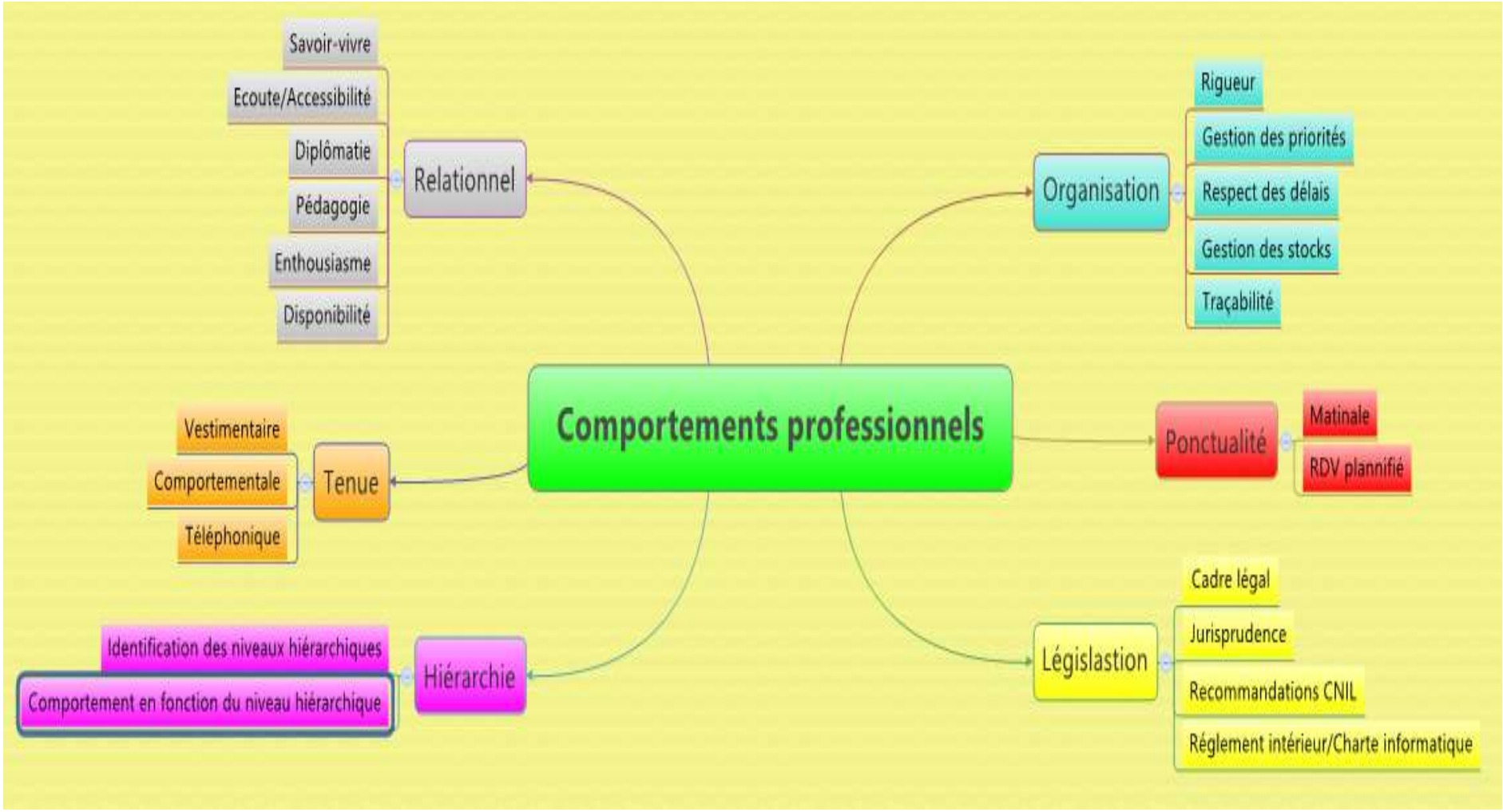
Nous travaillons en toute transparence avec nos clients c'est pourquoi il nous faut les connaitre. Nous proposons à chacun de nos clients des rencontres périodiques pour établir des bilans concernant notre prestation mais aussi pour comprendre leurs nouveaux besoins et leurs attentes à notre égard.

CONSEIL et FORMATION

Les compétences variées de HOTH INFO nous permettent de proposer des solutions adaptées et de former les utilisateurs finaux à ces technologies.

RAPIDITE

Chacun de nos contrats fait l'objet d'un accord concernant la résolution des incidents et les délais dans lesquels nous nous engageons à restaurer l'activité.


Comportements professionnels
Relationnel
Savoir-vivre
Ecoute/Accessibilité
Diplômatie
Pédagogie
Enthousiasme
Disponibilité
Organisation
Rigueur
Gestion des priorités
Respect des délais
Gestion des stocks
Traçabilité
Tenue
Vestimentaire
Comportementale
Téléphonique
Ponctualité
Matinale
RDV plannifié
Hiérarchie
Identification des niveaux hiérarchiques
Comportement en fonction du niveau hiérarchique
Législation
Cadre légal
Jurisprudence
Recommandations CNIL
Réglement intérieur/Charte informatique

ESTIMATION DE LA MASSE SALARIALE DE HOTH INFO

Calcul de masse salariale

	Salaire Net	Salaire Brut	Coût de revient	Nombre	Total	Coût horaire
TECHNICIEN et Assistante de direction	1400	1819	2583	9	23247	17,1
Ingénieur	2500	3247	4610	2	9220	30,53
Commerciale	1800	2337	3318	1	3318	21,9
Directeur	Fonction du bénéfice		5000	1	5000	
				Masse salariale	**40785**	

ESTIMATION DES FRAIS GENERAUX DE HOTH INFO

Calcul des frais généraux

	Prix	Nombre	Total
Location des locaux	2500	1	2500
Voitures(location)	400	3	1200
Voitures(essence)	100	3	300
Eau/Electricité	200	1	200
Internet	60	1	60
Téléphonie mobile	50	5	250
Renouvellement matériel	1500	1	1500
Consommable/Maintenance	500	1	500
		Frais généraux	**6510**

TOTAL MENSUEL : 47295 euros

Formulaire de contact Autoconcept

Nom et Prénom :

Service :

Courriel de contact :

Téléphone :

Catégorie de la panne : --Selectionner--

Priorité --Selectionner--

Détails de la demande :

Pièce jointe

Pièce jointe N°1

Pièce jointe N°2

Pièce jointe N°3

Formulaire d'intervention Autoconcept

Nom et Prénom :

Service :

Courriel de contact :

Téléphone :

Catégorie de la panne : --Selectionner--

Priorité --Selectionner--

Escalade : --Selectionner oui ou non--

Détails de la demande :

Interventions avec détails des intervenants et des dates :

Note interne :

Rouvrir le ticket ? : --Selectionner--

Si le ticket est rouvert, noter les détails de la panne :

Pièce jointe :

Pièce jointe N°1