PROJET SAS

2019

HighTech

BAUDVIN Vincent

DOUDANE Salima

ORTEGA Cédric

PAGES Bruno

ROL-MILAGUET Alexandre

cesi ÉCOLE SUPÉRIEURE DE L'ALTERNANCE

Présentation d'Autoconcept

*La société **AutoConcept** est un concessionnaire automobile située au 162 Route De Toulouse à Begles, elle possède un parc informatique de (70 à 80 postes) et comptabilise 83 salariés répartis en six services : le service atelier, le service comptabilité, le service véhicules neufs, le service d'occasion, et le service pièces de rechange.*

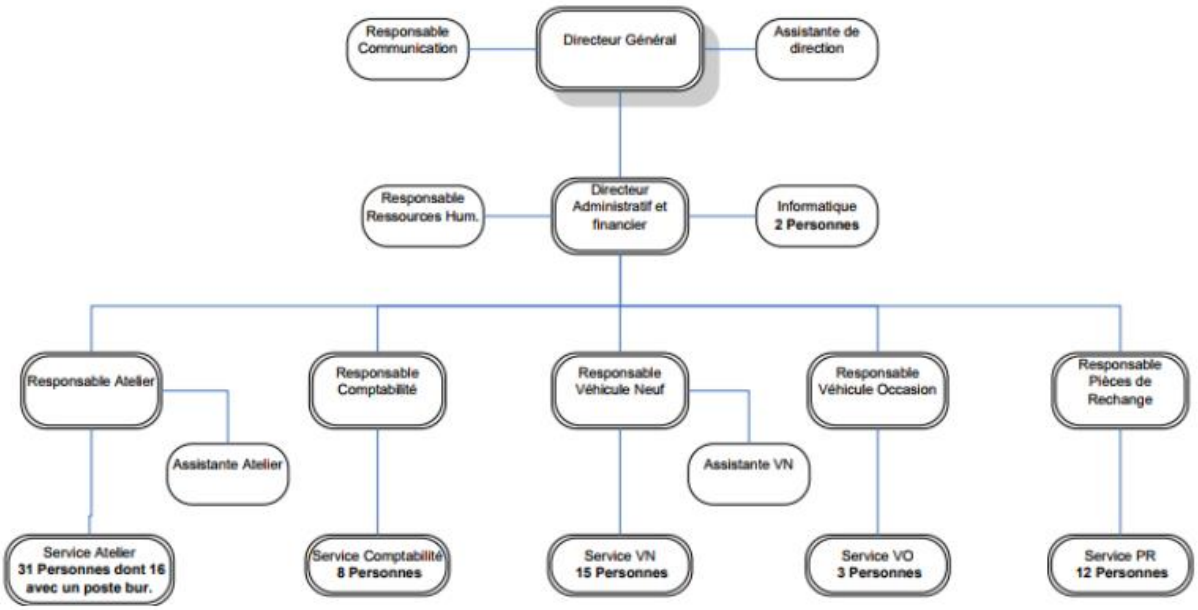
Cette société propose un service d'achat, de vente, et de reprise de véhicules neufs et d'occasions multimarques.

Un appel d'offre a été émis, car la société souhaite déléguer la gestion de son parc informatique à la suite de divers dysfonctionnements au sein de celui-ci. Au fil du temps, le concessionnaire c'est confronté à plusieurs obstacles liés à une mauvaise gestion du service informatique qui ont ralenti son avancée et grandement impacté sa productivité.

*Les derniers soucis en date relatés dans l'appel d'offre nous apprennent que la société a eu des soucis au niveau de la communication avec les informaticiens, de la disponibilité des postes ainsi que de la sécurité informatique. Au vu des éléments fournis par la société **AutoConcept**, nous proposons de fournir une solution sur mesure pour subvenir au mieux aux besoins de celle-ci avec pour but :*

- D'introduire une notion de confiance envers un Service Informatique coordonné et efficace.

- De proposer une solution de gérance de parc informatique simple et sécurisée.



Charte qualité service

Objectif de contrat

L'objet du contrat est de définir les modalités de gestion et d'interventions effectuées pour le compte du client. Ce contrat permet au client de disposer d'un service informatique coordonné et de proposer une formation aux usagers.
HIGHTECH® s'engagent à appliquer une clause de confidentialité, d'assurer une maintenance constante, un service continu et sécurisé, ainsi qu'un service d'assistance aux utilisateurs dit "**Helpdesk**" comprenant une interface logicielle et un standard téléphonique afin de mieux prendre en charge les demandes des utilisateurs.

Helpdesk

La création d'un "**Helpdesk**" permettra un suivi des demandes des utilisateurs, ainsi qu'un traitement efficace des tickets d'incidents. Le "**Helpdesk**" permettra notamment un contact direct et rapide avec le service informatique par le biais d'un standard téléphonique, ou par le biais de demandes informatiques réalisables via un logiciel préalablement installé sur chaque poste afin de hiérarchiser les demandes et traiter au mieux les incidents.
Afin de minimiser les coûts de la mise en place de ce système nous préconisons l'outil de Gestion libre de parc informatique (GLPI).
Les heures d'ouverture du service informatique, seront calquées sur les horaires de travail globaux des employés de **Autoconcept** (ex : du Lundi au Vendredi de 8h30 à 17h30). La procédure pour déclarer un incident commence par une demande informatique ou téléphonique comprenant la création d'un ticket d'incident qui sera ensuite traité par ordre de priorité par un technicien. La durée du traitement du ticket sera définie selon l'ampleur de l'incident. Le temps d'intervention dépendra du type et du domaine de la panne, puis enfin la durée de l'intervention sera déterminée par le technicien qui s'engagera à respecter les délais d'interventions prédéfinis.

Redéploiement des postes

Un redéploiement des postes de chaque service devra être effectué, chaque poste fixe et portable posséderont une version officielle de Windows 10 ainsi que des logiciels nécessaires à chaque service. Une image des postes sera sauvegardée afin de permettre une remise en service rapide en cas de besoin.

Sécurité informatique

Afin de sécuriser au maximum le parc informatique, les postes se verront attribués des restrictions afin d'empêcher toute installation ou manipulation hasardeuse par les utilisateurs. Nous préconisons aussi la mise en place de mot de passe sécurisés et renouvelés tous les 3 mois pour chaque utilisateur afin d'éviter toute intrusion et/ou fuite de données. Un parefeu ainsi qu'un antivirus sont aussi indispensables à la sécurisation des postes et des données contre toute intrusion ou contamination. De plus, un proxy sera mis en place en accord avec la direction et le C.E afin de restreindre, mais aussi de sécuriser la navigation sur internet. Pour toute installation de logiciel complémentaire une demande devra être effectuée au service informatique qui se chargera de celle-ci. Les utilisateurs se verront également formés aux bons usages liés à la sécurité informatique. Enfin la mise en place d'un accès WiFi public sera accessible aux personnes extérieures à l'entreprise afin d'empêcher toute connexion non autorisée à notre réseau.

Sauvegarde de fichier

Afin de minimiser la perte de fichier une sauvegarde sera effectuée quotidiennement. Les fichiers personnels devront être rangés dans un dossier prévu à cet effet et ne seront pas pris en compte dans les sauvegardes
La sauvegarde des postes portables s'effectuera de manière automatique lors de leurs connexions sur le réseau de l'entreprise.

Module d'évolution

Afin de palier au mieux à l'obsolescence informatique et d'amortir l'investissement d'**Autoconcept**, **HIGHTECH®** préconise l'achat de matériel neuf et récent, de marques fiables et avec une extension de garantie afin de pouvoir réparer et/ou remplacer au plus vite le matériel défectueux.
Si un renouvellement matériel doit être envisagé il suivra donc cette logique tout en restant dans un projet de continuité et d'évolution. Les remplacements ainsi que toute évolution du parc seront réalisés dans des délais raisonnables et ce sans gêner ou ralentir la productivité de l'entreprise.

Plan de Continuité d'Activité et Plan de Reprise d'Activité

Dans le cadre d'un **Plan de Continuité d'Activité** (**PCA**), **HIGHTECH®** veille à définir les architectures, les moyens et les procédures nécessaires pour assurer une haute disponibilité des infrastructures (matériel réseau, matériel de stockage, ...) supportant l'exécution des applications de l'entreprise. L'objectif est d'assurer que quel que soit la situation, les infrastructures mises en place garantissent aux utilisateurs un service ininterrompu et sécurisé.
Pour cela en cas de panne matériel notre service se tient prêt à agir au plus vite, de remplacer ou envoyer en réparation le matériel défectueux sans que cela ne paralyse l'utilisateur ou encore l'entreprise grâce à des « spares » (matériel de rechange), dans le cas contraire nous veillerons à ce que le relais soit automatiquement pris par le site secondaire de **HIGHTECH®**, assurant ainsi un **Plan de Reprise D'activité** (**PRA**) pour le redémarrage ordonné des applications en cas de défaillance ou de sinistre.
Le **PRA** définit les architectures, les moyens et les procédures nécessaires à mettre en œuvre pour assurer la protection des applications qu'il couvre. Son objectif est de minimiser l'impact d'un sinistre sur l'activité de l'entreprise.

Objectifs de reprise après incident en vue d'assurer la continuité de service grâce à l'automatisation de la sauvegarde et de la restauration, ainsi que de la réplication des données

---

HIGHTECH® s'engage à l'amélioration du fonctionnement et de la gestion de la sauvegarde, ainsi que de la disponibilité des données grâce à la mise en place d'un système de sauvegarde permettant la panne ou la casse d'un disque dur sans porter atteinte aux donnés qui seront aussitôt répliqués lors du changement de ce dernier. Nous proposons également un backup hebdomadaire complet sur l'un de nos serveurs ainsi qu'une utilisation optimisée du matériel et de l'espace de stockage en vue d'améliorer leur fiabilité , de garantir que les données et applications stratégiques demeurent opérationnelles et ainsi réduire les coûts d'exploitation en standardisant les processus grâce à une solution de continuité de service capable de fournir des méthodes de restauration cohérentes et adaptées à l'ensemble des employés, des processus et des technologies.

Sauvegarde

Matériels et solutions de stockage proposés

NAS
Afin d'améliorer la productivité ainsi que la sécurisation des données d'**Autoconcept**, il est indispensable pour notre entreprise de pouvoir mettre en place et configuré un serveur **NAS** (**Network Attached Storage**). Le **NAS** est un appareil de stockage de fichier doté de plusieurs disques durs et connecté à un réseau local (LAN).
Le **NAS** a pour vocation d'être accessible depuis des postes client à travers le réseau pour y stocker des données.

La gestion centralisée sous forme de fichiers à plusieurs avantages.

- Faciliter la gestion des sauvegardes des données d'un réseau.
- Prix intéressant des disques (HDD ou SSD) de grande capacité.
- Accès par plusieurs postes clients aux mêmes données stockées sur le réseau.

Organisation des services et gestions des droits d'accès chez le Client

Chaque service sera divisé en différents répertoire sur le **NAS**.
Ex :
Direction à répertoires 1,2,3,4,5
R H à répertoires 2,3,4,5
Comptabilité à répertoires 3,5
Vendeurs à répertoires 4,5
Tout le monde à répertoire 5

Tous les services seront sur le même réseau et auront donc un accès à un dossier commun afin de faciliter les échanges de données. En dépendant des droits hiérarchiques certains services auront les droits de lecture sur plusieurs répertoires.

Type d'architecture du NAS

HIGHTECH® propose un système de sauvegarde appelé "**RAID5**" qui combine l'utilisation simultanée des disques durs du **NAS**, profitant donc de performances améliorées en lecture/écriture, et d'une tolérance aux pannes. En cas de panne d'un disque dur il suffit de le changer et le logiciel intégré ainsi que les autres disques durs du **NAS** s'occuperont de reconstruire les données du disque endommagé.

Le stockage de données et les sauvegardes

Nous prévoyons de mettre en place un système de sauvegarde quotidien offrant la possibilité de récupérer les données perdues dans les dernières 24h. Elles seront en parallèle sauvegardées sur un site miroir qui garantira la haute disponibilité des données afin qu'un problème sur le **NAS** local ne soit pas fatal au bon fonctionnement des services.
Les sauvegardes automatiques seront quotidiennes, mais à tous moments les utilisateurs selon leurs droits d'accès pourront sauver manuellement des données sur leur répertoire dédié du **NAS**. Chaque jour les nouvelles modifications seront enregistrées et une sauvegarde hebdomadaire globale se fera à chaque début de semaine ce type de sauvegarde est dit "incrémentielle".
En accord avec la direction, et les différents droits d'accès utilisateur, nous pourrons assister au mieux **Autoconcept** et ses employés au tri et à la suppression d'anciennes données sur le **NAS**.
Chaque service ayant un répertoire dédié sur le **NAS** nous prévoyons de sensibiliser et de former les utilisateurs à travailler au mieux sur ces répertoires. Tous les éléments placés dans le dossier "documents" de leurs ordinateurs se verront également sauvegardés toutes les 24h sur le **NAS** et donc à tout moment ré-accessibles même en cas de panne matérielle.

La perte de données et les risques

Le système qui sera mis en place par nos services permettra de garantir à l'entreprise une perte de données quasi nulle et une accessibilité permanente à celles-ci ainsi qu'un fonctionnement continu des services.
Un service (Shadow Copy) sera également paramétré afin de permettre la récupération immédiate d'un fichier ou d'un dossier malencontreusement supprimé.
Le risque restant de perte de données se limitera dans le cas d'un sinistre total à moins de 24h (heure de la dernière sauvegarde sur le site miroir).

Les emplacements de sauvegarde

Tous les utilisateurs se verront doter d'un poste configuré au préalable et adapté à leur utilisation.
Ils seront tous configuré sur le NAS selon leurs droits d'accès afin de travailler directement depuis leurs répertoires et de sorte que les sauvegardes se fassent correctement sur les répertoires dédiés.
Les postes informatiques seront numérotés et triés par département selon la structure physique de l'entreprise.

Sécurité

La sensibilisation à la sécurité des usages professionnels et personnels

HIGHTECH® s'engage sur la sensibilisation des utilisateurs au bonnes pratiques liées à la sécurité informatique afin de minimiser les risques encourus.
Les conséquences d'une mauvaise sécurisation peuvent concerner les organisations, mais aussi la vie privée d'une ou plusieurs personnes, notamment par la diffusion d'informations confidentielles comme leurs coordonnées bancaires, leurs situations patrimoniales, leurs codes confidentiels, etc. De manière générale, la préservation des données relatives aux personnes fait l'objet d'obligations légales régies par la Loi Informatique et Libertés Consultable sur le site de la CNIL.
Certaines pratiques mettent également en péril la sécurité informatique de l'entreprise ainsi que les données personnelles des utilisateurs.

Exemples :

- Les connections sur des sites sensibles ou le téléchargement illégal.
- L'utilisation de matériel extérieur tel que les clés USB, les disques de stockage externe, etc.
- La connexion via Wifi, Bluetooth, etc, d'appareils personnels sur les réseaux de l'entreprise.
- La connexion à des réseaux publics et/ou non sécurisés avec des appareils de l'entreprise.

Nous disposons d'une charte ou toutes les informations seront communiquées et dûment signée par les employés après approbation de celle-ci par la direction et le comité d'entreprise.

Politique de confidentialité des informations personnelles, professionnelles et de services chez le client

Pour toute utilisation de données personnelles **HIGHTECH®** mettra à disposition sur chaque poste un dossier personnel qui ne sera pas compris dans les sauvegardes.
L'accès aux emails personnels ou à internet à usage personnel, seront décidés au préalable entre la direction de **Autoconcept**, son comité d'entreprise et le service informatique de **HIGHTECH®**.
Chaque employé devra signer une charte des sécurités des outils informatiques.

Politique de mot de passe

En ce qui concerne la politique des mots de passe **HIGHTECH®** préconise :

- Un mot de passe alphanumérique avec un minimum de 8 caractères avec au moins une majuscule et un caractère spécial.
- D'éviter les suites de nombres, de lettres, ainsi que les Noms ou encore les dates personnelles tel que son anniversaire.
- De changer les mots de passes tous les 3mois, sauf bien sûr si une intrusion survient sur un poste ou un répertoire entre temps, dans ce cas le ou les mots de passes seront immédiatement changés.
- De ne jamais donner son mot de passe.

Antivirus et pare-feu

Comme il a été rapporté que certains ordinateurs lançaient des alertes quant à la légalité de leurs logiciels il est important de prévoir le déploiement d'antivirus sur tous les postes ainsi que la configuration efficace d'un parefeu afin d'éviter toute contamination ou intrusion extérieure.

Ordinateurs portables

L'utilisation d'ordinateur portables professionnel hors du site et du réseau de Autoconcept comportent un risque élevé pour la sécurité et les données de l'entreprise. Pour cela nous proposons de chiffrer entièrement les disques durs de ces derniers ainsi que de mettre en place une sécurité supplémentaire de type VPN (réseau privé virtuel) pour que les connexions aux répertoires du NAS puissent se faire même hors site en toute sécurité.

CHARTE UTILISATEUR

Préambule

Les entreprises mettent en œuvre des systèmes d'information et de communication qui ne cessent d'évoluer, nécessaires à leurs activités, comprenant notamment un réseau informatique et téléphonique ainsi que des outils mobiles. Les salariés, dans l'exercice de leurs fonctions, sont conduits à utiliser ces outils mis à leur disposition et au service des entreprises.
L'utilisation de ces systèmes d'information et de communication doit se faire exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Dans un but de transparence à l'égard des utilisateurs, de promotion d'une utilisation loyale, responsable et sécurisée dans son ensemble, la charte pose des règles relatives à l'utilisation de ces ressources. Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation, non seulement pour la bonne exécution du contrat de travail des salariés, pour la sécurisation des données de l'entreprise et celle de leurs employés mais aussi vis à vis de la responsabilité pénale et civile de l'employé ainsi que celle de l'employeur. Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'entreprise.

Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information quel que soit leur statut, c'est à dire :

- Les dirigeants et mandataires sociaux
- Les salariés
- Les intérimaires
- Les stagiaires
- Les intervenants

Champ d'application

Chaque utilisateur est responsable de l'usage des ressources tant bien physiques que numériques. Nous parlerons donc ici de tout équipement mis à disposition tel que :

- Postes de travail
- Logiciels
- Outils collaboratifs
- Réseaux informatiques (NAS, routeur, connectique, internet, intranet, extranet...)
- Données informatisées (Mot de passe, fichiers, données et bases de données...)
- Périphériques (clef USB, Disque dur externe...)

Paramètres d'accès :

Les systèmes d'information et de communication (comme la messagerie électronique, la téléphonie, les sessions sur les postes de travail, le réseau et certaines applications ou services interactifs) sont protégés par des paramètres de connexion et d'authentification (identifiant et mot de passe).

- Toute session utilisateur est pourvu d'un mot de passe afin d'y accéder.

- Concernant le mot de passe, il est strictement personnel, il ne devra en aucun cas être communiquer à qui que ce soit, même sous demandes Hiérarchiques.

- Pour assurer la continuité de la sécurité, un changement de mot de passe sera à effectuer tous les trois mois.

- Lorsqu'il sera choisi par l'utilisateur, ce mot de passe devra être constituer d'au moins 8 caractères comprenant au minimum une majuscule, une minuscule, un chiffre et un caractère spéciale (+, %, -,ø,*,etc...).

- Il est fortement déconseillé d'utilisé le compte d'un collaborateur.

- Les ressources de l'Etablissement ne sont mises à disposition que du personnel précédemment cité. Elles devront être rationnelle aussi bien au niveau énergétique qu'au niveau des ressources physiques comme les impressions, …. Leur accès devra être refusé à toute personne extérieure à l'entreprise.

- L'utilisation d'internet doit respecter un cadre strictement professionnel.

- Un dossier portant la mention "personnel" ou "privé" peut être créer sur le disque dur du poste de travail et non sur un répertoire de l'Entreprise pour y stocker des documents ou mails privés pour une limitation de 10go de stockage par personne.

- L'utilisateur ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication de celle-ci.

Responsabilité de l'utilisateur :

- L'utilisateur s'engage à ne pas modifier, supprimer ou s'approprier des dossiers ou fichiers autres que ceux dont il est propriétaire. Le vol de données ou d'informations confidentiels dans le but de les revendre ou de les communiquer à un tiers sera soumis à de lourdes sanctions aussi bien sur le plan interne que pénal.

- L'utilisateur s'engage également à ne pas modifier, supprimer ou changer l'environnement de son poste de travail aussi bien physiquement (RAM, carte graphique...) qu'au niveau logiciel. Il est formellement interdit de supprimer ou modifier les softwares de l'entreprise ainsi que de désactiver l'Antivirus ou le pare-feu mis en place. Le service informatique se réserve le droit d'installer les logiciels nécessaires à l'environnement de travail et de désinstaller tout logiciel ou fichier non légal et/ou compromettant la sécurité ainsi que l'intégrité de l'entreprise.

- Chaque utilisateur est tenu au secret professionnel et à la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication, sont définies par la direction et applicables quel que soit le support de communication utilisé.

- L'utilisateur s'engage à se connecter au réseau uniquement avec les équipements fournis par l'entreprise et paramétrés par le service informatique. L'utilisation d'équipements personnels et connectés tel que smartphone, clef USB, disque dur externe, CD-ROM, carte SD […] est formellement interdit afin de lutter contre la cybercriminalité.

- En cas d'absence même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

- Chaque utilisateur doit appliquer le respect du secret professionnel et de la confidentialité des informations qu'il est amené à détenir, consulter ou utiliser. Les règles de confidentialité ou d'autorisation préalable avant diffusion externe ou publication, sont définies par la direction et applicables quel que soit le support de communication utilisé.

- Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication.

Internet

- Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurités ou de déontologie, l'accès à certains sites peut être limité ou prohibé par le service informatique (Facebook, Twitch, La française des jeux, …) qui est habilité à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant leur accès tel qu'un proxy.

- Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée.

- L'utilisation de la connexion Internet de l'entreprise ainsi que de son matériel à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite. Il est également prohibé de créer ou mettre à jour au moyen de l'infrastructure de l'entreprise tout site Internet à caractère personnel et/ou lucratif.

- De plus, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci.

- De même, tout téléchargement de fichier, en particulier de fichier média est prohibé, sauf justification professionnelle dûment validée par la hiérarchie.

- Il est rappelé à tous les utilisateurs qu'ils ne doivent en aucun cas se livrer sur Internet à une activité illicite ou portant atteinte aux intérêts de l'entreprise.

- Dans cette charte, ils sont informés que le service informatique enregistre leur activité sur Internet et que ces traces pourront être exploitées à des fins de statistiques, contrôle et vérification dans les limites prévues par la loi, en particulier en cas de perte importante de bande passante sur le réseau de l'entreprise.

Messagerie électronique :

- Chaque salarié dispose pour l'exercice de ses fonctions d'une boite Mails attribuée par la direction informatique.
- Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le service informatique des dysfonctionnent qu'ils constateraient dans ce dispositif de filtrage.
- Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber la productivité ainsi que de respecter les principes posés dans la présente charte.
- Ces messages doivent être signalés avec la mention "Privé" ou "Personnel" dans leur objet et être classés dès l'envoi dans un dossier lui-même nommé de la même manière. Ils devront donc être classés dès réception dans un dossier lui-même dénommé " Privé" ou "Perso".
- Toutefois, les utilisateurs sont invités dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne, pour l'envoi de message à caractère personnel plutôt que la messagerie de l'entreprise.
- Pour se protéger de l'hameçonnage et la fraude, l'utilisateur doit éviter autant que se peut de publier son adresse électronique sur Internet.
- Il doit faire preuve d'une vigilance accrue en cas de réception d'un message inhabituel ou douteux en provenance d'un expéditeur inconnu, présentant une syntaxe approximative, contenant des liens vers des sites et/ou des pièces jointes non sollicités ou encore contenant une demande afin d'effectuer des actions inhabituelles. Lorsqu'il pense avoir reçu un tel message ou s'il y a le moindre doute sur un message, il est tenu de ne pas y répondre et de le signaler immédiatement au service informatique sans tenter d'accéder aux liens contenus dans le message, d'ouvrir les pièces jointes associées ou de cliquer sur un lien hypertexte contenu dans le message.
- En raison des risques d'usurpation d'une adresse de messagerie, l'utilisateur doit faire preuve de discernement en cas de réception d'un message électronique qui semble provenir d'un responsable ou d'un tiers connu, lui demandant d'effectuer des actions inhabituelles ou non-conformes aux procédures internes. Dans ce cas, il doit vérifier verbalement auprès de cette personne le bienfondé de l'action (échange téléphonique, rencontre physique...).

Terminaux mobiles :

- Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe, d'un Ordinateur portable et d'un smartphone. Pour ce qui est de l'utilisation des terminaux mobiles en connexion, pour accès à des sites Internet ou à la messagerie électronique, les règles dictées ci-dessus s'appliquent de la même manière.
- Une connexion VPN sera fournie par l'entreprise pour les salariées nécessitant une utilisation d'un ordinateur portable hors-site. L'utilisateur sera donc connecté au réseau de l'entreprise et accédera à ses données via le NAS. Une sauvegarde sera appliquée dès la connexion de l'utilisateur.
- Il convient également que l'envoi de SMS soit réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel. Il est donc soumis aux mêmes règles rappelées plus haut.

- L'utilisation à caractère personnel du téléphone fixe ou mobile reste tolérée, à condition qu'elle reste dans les limites raisonnables tant en termes de temps passé que de quantité d'appels. L'utilisateur devra rembourser les surcouts pour l'entreprise engendrés par l'utilisation de la téléphonie à des fins personnelles tout particulièrement les appels à des numéros surtaxés et des appels passés depuis ou à destination de l'étranger.

- L'Entreprise s'engage à respecter la vie privée des Utilisateurs et à ne pas utiliser les données à caractère non professionnel identifiées comme telles dont elle pourrait avoir connaissance (Article L.1224-4 du Code du travail) et conformément à la loi RGPD.

- L'utilisateur est informé que le service informatique peut vérifier ou mettre à jour les paramètres de sécurité ou les applications et effacer à distance les données en cas de perte ou de vol de matériel connecté aux systèmes d'information de l'entreprise.

- L'entreprise se réserve le droit de mettre un terme à la mise à disposition du terminal mobile et de l'abonnement professionnel, ainsi que de sanctionner l'utilisateur en cas de négligences ou de malveillances constatées dans son utilisation.

Traitement de données à caractère personnel

- Un utilisateur qui reçoit ou accède à des données à caractère personnel, qu'il s'agisse de données relatives aux collaborateurs de l'Entreprise ou à des tiers (clients, partenaires, candidats...), s'engage à respecter strictement la réglementation applicable, la Politique de protection des données personnelles de l'Entreprise ainsi que les procédures associées au traitement de ces données.

- Conformément à la réglementation applicable en matière de données à caractère personnel, les Utilisateurs sont informés qu'ils disposent d'un droit d'accès et de rectification relatif à l'ensemble des informations personnelles les concernant, ainsi qu'un droit d'opposition pour motif légitime du traitement de ces données.

- L'utilisateur peut exercer ces droits en contactant la personne désignée par l'Entreprise ou à défaut le service des Ressources Humaines de l'Entreprise.

Contrôle des activités

Contrôles automatisés

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Ces traitements permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Sont notamment surveillées et conservées les données relatives :

- À l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications et suppressions de fichiers.

- Aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, afin de détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion ainsi que les activités telles que la consultation de sites ou les téléchargements de fichiers.

- Au contrôle de leur activité ainsi que de leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

- Il est précisé que chaque utilisateur pourra avoir accès aux informations enregistrées lors de ces contrôles le concernant sur demande préalable à la direction.

- De plus, les fichiers journaux énumérés ci-dessus sont automatiquement détruits dans un délai maximum de 6 mois après leur enregistrement.

Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs
Le contrôle concernant un utilisateur peut porter sur les fichiers contenus sur le disque dur de l'ordinateur, sur un support de sauvegarde mis à disposition, sur le réseau de l'entreprise, ou encore sur sa messagerie. Sauf risque ou événement particulier, la direction ne peut ouvrir les fichiers ou messages identifiés par l'utilisateur comme personnels ou liés à la délégation de personnel conformément à la présente charte sauf en présence de l'utilisateur ou un délégué du personnel représentant l'utilisateur concerné (nommé par celui-ci).

Information et sanctions

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié dès son entrée dans l'entreprise.
Le service informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur les procédures de sauvegarde et de filtrage.
Elle les informe régulièrement sur l'évolution des limites techniques du système d'information et de communication ainsi que sur les menaces susceptibles de peser sur la sécurité.
Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par la direction informatique dans le cadre de la présente charte.
En cas de besoin, les salariés pourront être formés par le service informatique pour appliquer les règles d'utilisation du système d'information et de communication prévues.
Le manquement aux règles et mesures de sécurités décrites dans la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires proportionnées à la gravité des faits concernés.
Dans ce dernier cas, les procédures prévues dans le règlement intérieur et dans le Code du travail seront appliquées.
L'utilisation reconnue à des fins personnelles de certains services payants à travers le système de communication de l'entreprise ou son représentant légal, se réserve également lieu à un remboursement de la part de l'utilisateur concerné.
Le représentant de l'Entreprise ou son représentant légal, se réserve également le droit d'engager ou de faire engager des poursuites pénales indépendamment des sanctions disciplinaires mises en œuvre, notamment en cas de fraude informatique, de non-respect des droits d'auteur ou de violation du secret professionnel.

En cas de violation de la charte, l'employeur se réserve de prendre des sanctions disciplinaires à l'encontre du salarié. Cependant, celles mentionnées dans ladite chartre couplée au règlement intérieur ne doivent pas être contraires aux règles prévues par le Code du travail Article L1121-1 ni posséder un caractère disproportionné.

La charte informatique permet également à l'employeur de rendre l'abus plus facilement opposable au salarié en cas de litige porté devant les tribunaux, notamment en cas de licenciement. Dans ce dernier cas, la violation de la charte est prise en compte par les juges et permet ainsi d'appuyer la sanction prise par l'entreprise en cas de violation des règles qu'elle contient.
La charte doit être validée par la direction, le CSE, et une copie doit être envoyée au prudhomme ainsi qu'à l'inspection du travail.
(Ci-joint une clause de confidentialité à dater et signer et à remettre en main propre).

Mémo interne destinée aux techniciens de HIGHTECH® :

Lors d'une intervention vous vous devez de respecter les règles exigées par notre société car en vous rendant auprès de nos clients vous reflétez notre image de marque.

Ces règles doivent être obligatoirement suivies pour le bon déroulement de vos interventions. En cas de manquements rapportés par un de nos clients vous vous exposez à un rappel à l'ordre voire à l'application d'une sanction.

Certains de nos clients ont transmis récemment à nos services les remarques suivantes :

- Tenue vestimentaire non professionnelle des informaticiens : « un matin, l'un d'eux est arrivé en jogging pour dépanner un poste alors qu'un commercial était avec un client ».
- Langage incorrect tenu par un des informaticiens : Réponse de manière déplacée à la demande d'un utilisateur de le dépanner.

D'autres remarques ont été recensées tel que : certaines versions de logiciels illégales, règles de confidentialité bafouées, ou encore des retards des techniciens lors d'interventions.

Tout technicien doit, quelle que soit sa fonction ou sa spécialité, apporter son aide d'urgence à un utilisateur dont le problème pourrait ralentir la productivité ou mettre en péril la pérennité de son entreprise.

En cas de difficulté aiguë, le technicien ne peut abandonner son client, à moins que celui-ci ne fasse preuve d'un comportement belliqueux.

Le secret professionnel s'étend à tout ce que le technicien a vu, connu, appris, constaté, découvert ou surpris dans l'exercice de ses fonctions.

Lors de l'appel d'un client un pré-diagnostic doit être réalisé afin de cerner le problème rencontré et un ticket d'incident doit être créé. Un rendez-vous sera fixé avec le client en fonction de ses disponibilités dans un délai maximal de 48 heures. Un mail ou un SMS de confirmation sera envoyé récapitulant la date et l'heure du rendez-vous ainsi que les informations complémentaires au sujet de l'intervention.

Dans le cas d'une demande via l'Helpdesk, le technicien se doit de classer et de hiérarchiser au plus vite la demande selon le domaine et la gravité de l'incident.

Les tickets doivent être traités au plus vite et ne doivent pas s'accumuler.

Le technicien s'engage à être courtois et à utiliser un langage écrit correct comprenant les formules de politesse adéquate.

L'utilisateur doit être prévenu sur la prise en charge du ticket et si la résolution de l'incident venait à bloquer son poste de travail il est impératif de le prévenir à l'avance pour convenir d'un horaire d'intervention ne le pénalisant pas dans son travail. Dans le cas où son poste se retrouverait bloqué pour une durée indéterminée il convient de lui trouver une solution de remplacement afin de ne pas nuire à son travail ainsi qu'à la productivité de l'entreprise.

HIGHTECH® ainsi que ses techniciens s'engagent à :

- ✓ *Garantir la qualité de l'accueil réalisé sur place.*
- ✓ *Analyser la demande et de proposer la ou les solutions techniques les plus adaptées aux besoins du client.*
- ✓ *Tout faire pour aider le client face à son problème technique.*
- ✓ *Obtenir la satisfaction du client.*
- ✓ *Remettre une facture détaillée au client.*
- ✓ *Faire le suivi de la satisfaction après chaque intervention (contrôle Qualité).*
- ✓ *Répondre aux réclamations (contrôle Qualité).*
- ✓ *Préserver la confidentialité des données du client.*
- ✓ *Assurer une protection adéquate du matériel, des logiciels ainsi que des données.*

ATTITUDE

- → Une tenue vestimentaire adéquate.
- → Être poli et courtois.
- → Être attentif et consciencieux.
- → Apporter des réponses fiables et compréhensibles.
- → Agir avec professionnalisme et réactivité.
- → Accueillir nos clients dans le respect des règles de confidentialité.
- → Établir une relation personnalisée.
- → Avoir une écoute attentive et répondre aux questions de manière à être compris.

PONCTUALITE

- → Se présenter 10-15 minutes en amont lors d'une intervention.
- → Respecter le planning et les horaires des rendez-vous fixés.
- → Ne pas déplacer de rendez-vous sans le consentement du client et sans en avertir sa hiérarchie.
- → Prévenir en cas de retard (Client et HIGHTECH®).

CONCLUSION

Suite aux différentes problématiques rencontrées par **Autoconcept** vis-à-vis de la gestion de son parc informatique, un mémo adressé aux techniciens ainsi qu'une charte utilisateur ont été créés afin de solidifier notre action sur le long terme. Répondant à des problèmes comme la sauvegarde, la sécurité, la qualité de service, la formation des utilisateurs, et la légalité du parc informatique, **HIGHTECH®** propose un service complet engageant un minimum de frais ou de modifications majeures nécessaires au bon fonctionnement de l'infrastructure numérique d'**Autoconcept**. La plupart de notre action se base sur la mise aux normes et la mise en place de bonnes pratiques visant à éliminer ou du moins à minimiser les différents problèmes rencontrés et rapportés par l'entreprise.