CESi entreprises
FORMATIONS EN ENTREPRISE ET ALTERNANCE

Projet SAS

GMSI 31

Gestion et maintenance de parcs informatiques

Chef de projet : FAVERO Jeremy
Équipe projet : YILMAZ Alexandre, PIRES Michael

Remerciement

Nous tenons à remercier le CESI ainsi que l'instituteur de ce projet, Christian DEMAY.

Nous tenons également à remercier Thimothée Gury et Matheo CHEVILLON pour leurs aides et leurs conseils lors du lancement du projet.

Sommaire

Alt
F4 PC

Avant-Propos

Dans le cadre de nos études au CESI de Nancy, il nous a été confié la création de ce projet nommé SAS.
Les objectifs pédagogiques sont :

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

Notre objectif est de travailler en équipe, pour cela nous utiliserons :

- Des outils de communications efficaces (Microsoft Teams, Discord)
- Des outils administratifs (Google Docs, Excel)
- Des outils de réalisation artistique (Photoshop, ...)

Étude de l'existant

1. Présentation

AutoConcept est un concessionnaire disposant d'un parc informatique d'un peu plus de 80 postes et de 83 salariés de la société sont répartis en différents services classés.
L'entreprise souhaite externaliser les prestations informatiques et confier la gestion de son parc informatique à une entreprise de prestation informatique AutoConcept possède déjà un service informatique composé de 2 techniciens. Dans le cadre de notre offre, un des deux techniciens sera recruté au sein de AltF4Pc
Le concessionnaire a réparti ces effectifs de la manière suivante :

- Une majorité au Services Atelier *(~30 personnes)*
- Une partie au Service VN *(15 personnes)*
- Une autre partie au Service PR *(12 personnes)*
- Un nombre plus faible au Service Comptabilité *(8 personnes)*
- Peu de personnes au Service VO *(3 personnes)*
- Quelques informaticiens dont un recrutable *(2 personnes)*
- Le reste du personnel dans le pôle administratif

<u>Problématique Auto concept</u>

Après un audit de la société AutoConcept et le retour de son service commercial, nous avons pu relever plusieurs points à traiter :

Technique et Matériel

Pour commencer nous allons aborder les points techniques. La société nous a présenté des soucis matériels (crash de disque dur, lenteur du matériel). Après notre analyse et le retour commercial nous avons noté :

- Pas de mesures immédiates de sauvegarde (chaque utilisateur sauvegarde son travail sur son poste)
- Licences Logiciel obsolète ou piraté (Licence Windows)
- La sécurité est inexistante (aucune sécurité de constatée, pas de mot de passe, pas de cryptage des fichiers sensibles, tout le monde a accès à tous les postes de la société)

Employé et Clientèle

La société n'a rien mise en place sur le normes et réglementation lié aux activités numériques que ce soit pour ses employés ou sa clientèle.

- Charte d'utilisation informatique
- Productivité
- Norme RGPD
- Règles de sécurité informatique et Télécoms
- Règles régissant l'utilisation des moyens informatiques mis à disposition des salariés
- Règles régissant la mise en place d'une solution de filtrage de contenus en entreprise.

Economique

Partons maintenant sur un sujet que les dirigeants et les comptables aiment regarder de près, les coûts et ses possibles réductions,

- Pas de chiffrage des coûts (le client ne sait jamais quand son matériel sera de retour et combien cela va lui coûter)
- Amortissement du matériel sur 3 ans voulu par le service commercial
- Le contrat de garantie matériel n'est plus à jour et ne correspond plus aux attentes de AutoConcept (économie possible avec un contrat mise à jour)
- Prestation Externe (économie de 2 postes de technicien)

<u>Attente de prestations</u>

Après avoir écouté le service commercial de Auto concept nous avons pu constater que le client souhaite :

- Délais d'intervention réduit (réactivité pour la résolution de problèmes, remplacement de matériel)
- Hotline disponible.
- La continuité de service en cas de panne est inexistante
- Bon relationnel général avec le prestataire.
    - Présentation et qualité des intervenants (Tenue, écoute, diplomatie, pédagogie, réactivité, polyvalence, autonomie soin et minutie. etc.)
    - Confidentialité (client sensible au vol de données)
    - Système de garantie efficace (remplacement du matériel par équivalent a minima)
- Savoir rendre compte de son activité
- Rigueur et méthodologie
- Savoir planifier et organiser la charge de travail
- Intégration des logiciels de l'entreprise

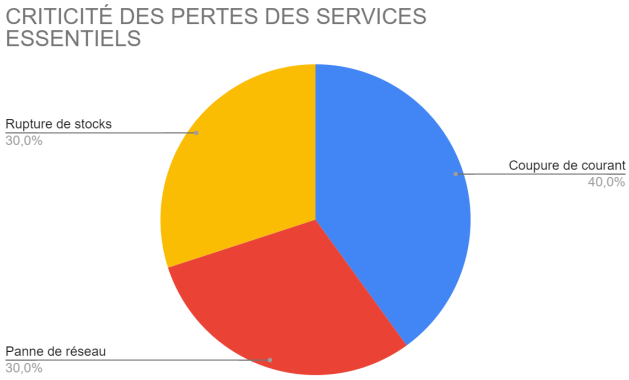
Alt F4 PC

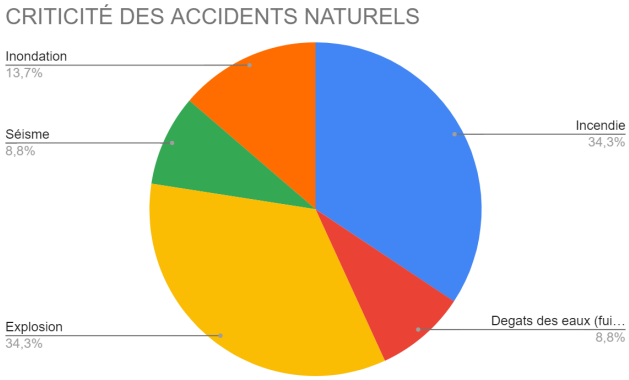
Après étude des problématiques nous avons pu approximativement chiffrer les coûts actuels de la société Auto concept :

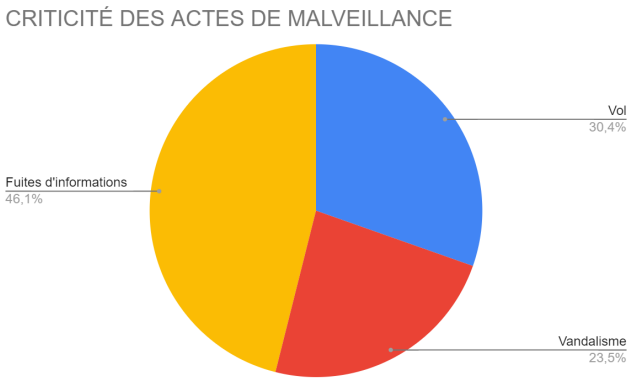
Problématique	Perte d'exploitation	Pourquoi ?
Matériel	80 000 €	Matériel vétuste
Sauvegarde	50 000 €	Perte de chance de conclure une vente
Sécurité des données	50 000 €	Perte de chance de conclure une vente
Mots de passe	50 000 €	Perte de chance de conclure une vente
Délai de SAV	60 000 €	Perte de chance de conclure une vente
Logiciels non essentiels	17 600 €	Une perte de productivité de 220 euros par poste de travail
Logiciels piratés	150 000 €	Microsoft sanctionne ainsi les utilisateurs de Windows en version non officielle
Accessibilité des données	3 510 000 €	Estimation d'IMB Security dans l'étude de 2018
Lenteur du matériel	96 000 €	En supposant que chaque poste perd 15 min par jours
Garantie pour matériel non présent	36 000 €	80 % des entreprises ont des garanties pour du matériel qu'ils n'ont plus, en estimant qu'il paye 300 € par mois par poste * 10 postes non présents pour exemple
Perte de confiance des clients	12 000 €	En supposant que chaque jour un client est déçu par les délais et le sérieux de la concession

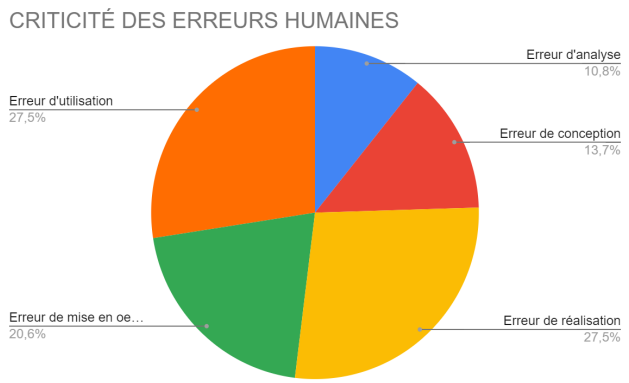
Total des pertes en euro (€)	**4 111 600 €**	

Après études des risques encourus par l'entreprise, voici ce qu'on observe







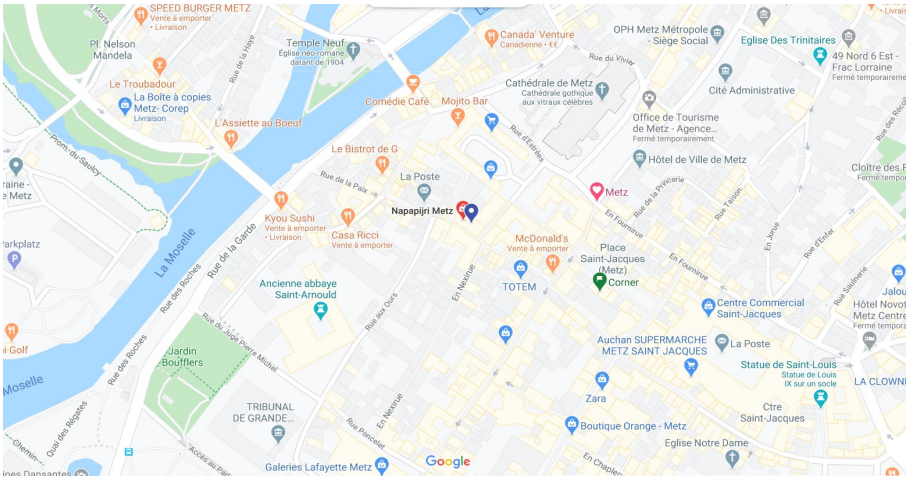


Présentation de l'entreprise :

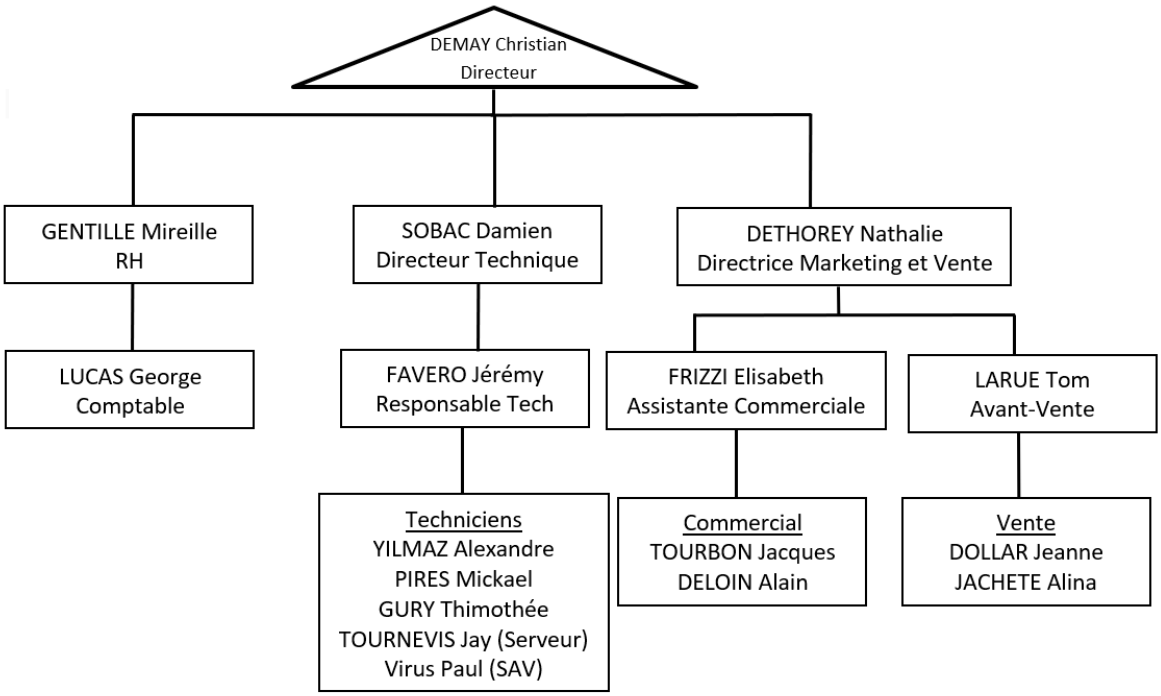
Historique : Création en 1998 au cœur de la ville de Metz

Altf4PC a fait de la maintenance de parcs informatiques son cœur de métier pour accompagner les entreprises et les particuliers dans la révolution numérique.

Raison sociale :	Alt F4 PC
Adresse :	25 rue du palais 5700 Metz
Tel:	03 87 50 51 52
Mail:	contact@altf4pc.fr
Site Web:	www.Altf4maintenance.com
Horaire :	9H-12H / 14H-18H du lundi au vendredi
Statut juridique :	SARL
Capital :	50000
Effectif :	9 personnes
Activité :	Gestion et maintenance de parcs informatiques
Siret :	255 255 255 255



Organigramme hiérarchique



Nos Solutions

Un technicien dédié sur site qui sera votre interlocuteur privilégié avant escalade à nos services. Après l'étude de votre dossier, voici ce que notre société est en mesure de vous proposer, nous avons classé vos problématiques dans quatre catégories,

Les accidents naturels

Dans ce domaine Alt F4 PC vous propose de bien définir les emplacements de vos future installations sensible (type serveur) de préférence dans une pièce close protégée des risques d'incendies et des explosions au premier étage de votre entreprise ce qui réduira grandement les risques de dégât des eaux. Accompagnez ceci d'un système de prévention incendie (détecteur de fumée)

Les pertes essentielles de services

Dans ce domaine plusieurs pistes d'améliorations sont possibles, équiper vos installations les plus critiques avec un onduleur afin d'éviter la coupure immédiate de votre système et de maintenir son fonctionnement en cas de coupure d'électricité courte, de permettre en cas d'anomalie plus grave de laisser le temps au système de sauvegarder vos informations sans risque de perte.

Pour garder une continuité de connexion sur internet plusieurs solutions s'offrent à vous. (Doublement de votre ligne, basculement de la connexion via le réseau 4G).
Enfin pour ne plus manquer de fournitures nous préconisons la mise en place d'un logiciel de gestion des stocks (GLPI)

Le technicien ALTF4PC sera en charge de la gestion des stocks sur site et pourra intervenir plus efficacement en cas de besoins.

Mise en place au sein d'AUTO CONCEPT d'un stock matériel de 15% du Parc de l'entreprise (poste de travail, Ram, disque dur, consommables...)

Les erreurs humaines

Nous vous accompagnerons lors de la réalisation de ce projet et nous validerons avec vous toutes les étapes essentielles de son développement, nous garantissons la prise en charge et de la conception du projet, ainsi que de la réalisation et de sa mise en œuvre. Nous réaliserons pour vous la formations et la prévention de votre personnel à l'usage de l'outil informatique.

La malveillance

Pour les actes de vol et de vandalisme plusieurs solutions sont actuellement possibles, comme la sécurisation des postes fixes, la mise en place d'une alarme dans la salle serveur et rendre responsable le personnel disposent de matériel nomade (téléphone, PC portable) ;

Nous vous proposons aussi toute un catalogue de solution pour le renforcement de la sécurité de votre outil informatique, comme l'interdiction d'installation de logiciel tier, la mise en place d'un système de contrôle de trafic ou la mise en place de mot de passe ...

Tableau récapitulatif des risques et ses solutions

Catégories	Risques	Probabilité	Niveau d'impact	Criticité	Solutions
Accidents naturels	Incendie	4	4	16	Prévention, mise en place de systèmes anti-incendie
	Dégâts des eaux, inondation	2	3	6	Préféré l'installation des équipements sensible à un étage protection des installations
	Explosion	4	4	16	Préféré l'installation des équipements sensible loin des produits inflammable
Pertes de services essentielles	Coupure de courant	4	2	8	Installation d'onduleur sur les serveurs pour permettre la sauvegarde des données
	Panne de réseau	2	3	6	Installation d'une seconde ligne ou d'un modem 4G en cas de coupure de la ligne principale réseau
	Rupture de stocks	3	2	6	Investir dans une solution de gestion de stock
Erreurs	Erreur d'analyse	3	1	3	Mise en place d'une procédure de vérification
	Erreur de conception	1	4	4	Mise en place d'une procédure de vérification
	Erreur de réalisation	2	4	8	Mise en place d'une procédure de vérification
	Erreur de mise en œuvre	2	3	6	Préparation de la mise en œuvre en amont
	Erreur d'utilisation	4	2	8	Formation des utilisateurs à l'utilisation de l'outil informatique, actions de prévention
Malveillance	Vol et vandalisme	4	2	8	Fixation du matériel, câbles antivol informatiques, alarmes
	Fuites d'informations	4	3	12	Prevention, renforcement de la sécurité, adapter les profils utilisateurs en fonction des besoins,

Réévaluation des risques après la mise en œuvre de la solution proposé par Alt F4 PC

Nous pouvons constater une nette amélioration des risques quelques soit le domaine abordé.

En conclusion nous pouvons dire qu'avec la mise en place de mesure simple et plus ou moins coûteuse, la productivité et la sécurité informatique de l'entreprise peut être grandement améliorée. Ce qui nous amène aux bénéfices financer de la mise en place de la solution que nous vous proposons. Lors notre étude de cas nous avons estimé une perte approximative de 4 000 000 €. La mise en place de la solution vous permettrez de faire une économie de 60 % environ. Ce que nous allons vous détailler dans cette partie.

	Perte d'exploitation	Pourquoi?	Solutions	Avec notre solution
Materiel	80 000 €	Matériel défectueux	Audit matériel et remplacement si nécessaire	26 400 €
Sauvegarde des données	50 000 €	Perte de chance de conclure une vente	Cloud / serveurs	16 500 €
Sécurité des données	50 000 €	Perte de chance de conclure une vente	Profil d'accès au parc informatique	16 500 €
Mots de passe	50 000 €	Perte de chance de conclure une vente	Politique de mot de passe obligatoire	16 500 €
SAV	60 000 €	Perte de chance de conclure une vente	Garantie de continuité du service, contrat adapté à vos besoins	19 800 €
Logiciels tiers	17 600 €	un gaspillage de 220 € par poste de travail	Gestions et blocage des logiciels tiers	5 808 €
Logiciels non officiels	150 000 €	Microsoft sanctionne ainsi les utilisateurs de Windows en version cracked	Achat de licence logiciel officiel et uniformisation du parc logiciel	49 500 €
Accessibilité à l'outil informatique	3 510 000 €	IMB Security dans l'étude de 2018	Mise en place d'une politique de profil et mot de passe	1 158 300 €
Obsolescence du matériel	96 000 €	en supposant que chaque poste perd 15min par jours	Remplacement du matérielle, nettoyage réseaux, bande passante, QOS améliorer	31 680 €
Contrat de garantie	36 000 €	80% des entreprises ont des garanties pour du matériel qu'ils n'ont plus, en estimant qu'il paye 300€ par mois par poste * 10 postes non présents pour exemple	Gestion des stocks + réévaluation des contrats	11 880 €
Confiance de la clientèle	12 000 €	en supposant que chaque jour un client est déçu par les délais et le sérieux de la concession	Communication grande publique et une prestation du prestataire informatique sans reproches	3 960 €
Perte totale (€)	4 111 600 €		Avec notre solution	1 356 828 €

Locaux de stockages :

Installation des différents serveurs (Stockages, Sauvegarde, Licence, etc...) dans un local spécialement dédié. Cette salle devra comprendre :

- Un sol surélevé pour permettre le passage de fibre optique, câble d'alimentation, de réseau, de téléphonie,
- Différents systèmes de contrôle et d'alerte : 'onduleur de secours en cas de coupure de courant
- Climatisation dans la salle Baie de stockage
- Verrouillage de l'accès à cette salle (clé, digicode ou badge)

Objectif : Sécuriser le matériel réseau et les données informatiques.

Sécurisation du réseau :

- Mise en place de filtrage de données (pare-feu) pour privatiser le réseau informatique et éviter toute intrusion dans le système.
- Mise en place d'un système de partages privatisés par service.
- Politique de mots de passe
- Uniformisation du Parc informatique (logiciels, postes, licences...)

Parc Informatique :

- Uniformisation et maintenance du Parc informatique (logiciels, postes, licences, garanties…)
- Politique de mots de passe
- Sécurisation des postes de travail (câble antivol, anti intrusion USB, proxy…)
- Bitlocker (cryptage des données postes)

Objectif : Permettre un contrôle des données et des accès des différents utilisateurs.

Gestion des Stocks :

- Technicien en charge de la gestion des stocks (matériels, licences, consommables…)
- Stock matériel dédié AutoConcept

Services :

- Formation du personnel à l'outil informatique
- Rédaction d'une charte de la bonne utilisation de l'informatique en entreprise
- Intervention à J+2 heures sur site
- Hotline 5/7j Astreinte du week-end (numéro dédié)

Plan de sauvegarde de données

Plan de sauvegarde N°1 :

Le *NAS10* :
Un serveur NAS (Network Attached Service) est une solution de gestion de données optimale pour les PME car il est spécialement conçu pour un parc informatique moyen.
Le principal désavantage du NAS pour l'entreprise est le ralentissement causé par la mise en réseaux des ordinateurs. C'est pour cette raison qu'il est adapté à un petit ou moyen parc informatique.
Un NAS vous offre un volume de stockage très important selon le RAID choisit (RAID 1, RAID 5, RAID 10… *cela correspond au nombre de baies pour les disques durs*) et vous permet de centraliser tous vos documents et fichiers multimédias sur un support unique, facilitant ainsi l'accès et le partage. Il est accessible depuis n'importe quel ordinateur ou appareil mobile tant qu'ils sont sur le même réseau. Et en plus de proposer une capacité de stockage étendue, vous ou tout autre utilisateur autorisé peut avoir accès à son contenu depuis n'importe où pourvu qu'une connexion internet soit disponible.

Pourquoi choisir le NAS pour votre entreprise ?

L'installation NAS est devenue la solution de stockage la plus répandue dans les TPE ou les PME telle que la vôtre.

Elle permet d'éviter la perte de données en installant un RAID 1. Elle permet également le travail en collaboration car le NAS est configuré en réseau sur chaque poste et permet donc le partage de fichiers.

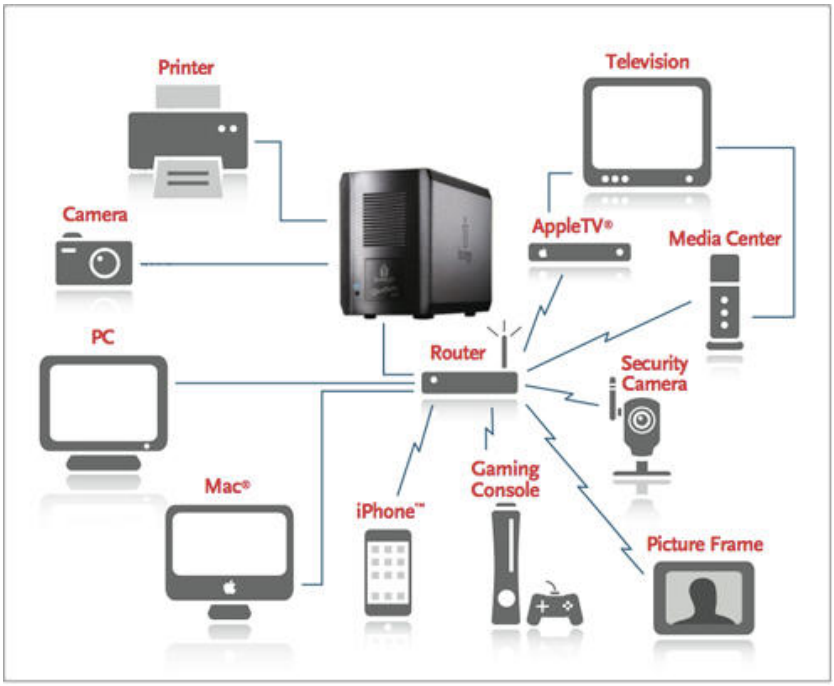
Les constructeurs de NAS peuvent intégrer des logiciels lors de la configuration du NAS comme ceux qui permettent leur administration globale.

En vous proposant un NAS Qnap TS-128A, il vous offre une interface web des plus performantes qui permettra non seulement de gérer l'accès à vos données, d'automatiser la sauvegarde vers le Cloud grâce au logiciel intégré, de créer une virtualisation d'un système d'exploitation « Windows Serveur » et beaucoup d'autres options que nous pouvons vous faire découvrir.

Qnap possède une interface web simple et visuelle proposant de nombreuses applications comme :

- La sauvegarde et la restauration des données.
- *Cloud Sync* : Pour la synchronisation avec le Cloud.
- *Directory Serveur* : Administration et droits d'accès aux dossiers/fichiers.
- *Gestionnaire de stockage* : Pour la configuration du RAID et pour surveiller l'état des disques durs.
- Centre de mises à jour.
- *Le centre de packages* : Pour installer de nouvelles applications proposées par Synology

L'avantage de ce Raid 2 est de vous proposer un stockage de 32To pour un prix relativement bas (~150€) comparé à beaucoup d'autres. Possédant 2 USB supplémentaires vous pouvez aisément brancher deux imprimantes directement dessus.



Mise en place d'une sauvegarde automatique :

Sauvegarde des données à risque sur les serveurs tous les soirs à partir de 23h. Sauvegarde de toutes les données du réseau de la semaine le vendredi soir à partir de 23h

Sauvegarde de toutes les données présentes sur le réseau le mois précédent le 1er samedi du mois à 23h

La sauvegarde du mois sera à sortir du sein de l'entreprise pour permettre d'avoir une sauvegarde en cas d'incident dans les locaux de l'entreprise (feu, inondation, etc..).

Les données seront aussi sauvegardées en double sur un serveur situé à un autre endroit dans l'entreprise, pour permettre d'avoir une sauvegarde de secours en cas d'incident dans les locaux de l'entreprise (feu, Inondation, etc..).

Objectif : Permettre de retrouver les données de l'entreprise les plus récentes possibles en cas d'incident sur les serveurs.

Note de Synthèse

L'informatique est de plus en plus présente dans les entreprises, cela pourrait devenir un problème. Celle-ci expose plus que jamais les données critiques de l'entreprise à un risque. Il nous faut pour cela des lois et des règles nous permettant de protéger nos données et nos utilisateurs. Voici donc quatre grands points qui nous intéressent :

Quelles sont les règles régissant l'utilisation des moyens informatiques mis à disposition des salariés ?

Pour les juges, les consultations de sites Internet pendant le temps de travail et grâce à l'outil informatique mis à sa disposition par l'entreprise, sont présumées avoir un caractère professionnel de sorte que l'employeur peut les rechercher aux fins de les identifier même en dehors de la présence du salarié.

Cela vous autorise à inspecter le disque dur de l'ordinateur du salarié, à son insu, pour voir ce qu'il a téléchargé.

Dans le même ordre d'idées, vous pouvez accéder à la liste des favoris de l'ordinateur professionnel du salarié sans l'en informer au préalable, l'inscription de sites Internet dans la liste des favoris de l'ordinateur professionnel du salarié ne leur confère aucun caractère personnel.

Source : Cour de cassation, civile, Chambre sociale, 9 juillet 2008, n° 06-45800

Le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans suivre l'article 34 de la loi n° 78-17 du 6 janvier 1978 (l'article 34 est celui présenté dans le point suivant) est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Source : Article 226-17 du code pénal

On peut en conclure que tant que ce sont des données professionnelles, l'entreprise n'a pas besoin de la présence du salarié mais que dès nous accédons à des données personnelles celui-ci est indispensable.

Quels moyens doivent être mis en œuvre pour la sécurité des fichiers ?

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.

Source : Article 34 de la loi informatique et libertés

L'entreprise doit donc prendre toutes les mesures utiles et nécessaires à la protection à la sécurisation des données et des fichiers.
Pour cela de nombreuses formes de sécurité sont apparues au fur et à mesure avec pour intention une sécurité des plus forte.
Voici quelques exemples :

- Politique de mot de passe.
- Une charte informatique.
- Disposer d'une cartographie précise de l'installation informatique et la maintenir à jour.
- Disposer d'une liste des utilisateurs ayant des accès privilégiés.
- Gérer les procédures d'arrivée et de départ des utilisateurs.
- Limiter les accès de l'entreprise à Internet au strict nécessaire pour pouvoir facilement centraliser et rendre homogène la surveillance des échanges.
- Inciter les utilisateurs à ne pas connecter leurs équipements personnels au système informatique de l'entreprise.

Quelles informations doivent être portées aux personnes dans l'entreprise concernant l'utilisation des outils informatiques ?

La charte informatique est conseillée afin d'apporter les informations nécessaires à l'employé. De plus celle-ci est :

- Un concept admis par tous : dans la loi, dans le droit, dans la jurisprudence, dans les recommandations CNIL...
- Elle limite les responsabilités pénales et civiles au vu de deux articles du code civil (Art 1383 et 1384) et un article du code pénal (art 121-2).
- Et évidemment parce que la charte informatique est obligatoire à partir du moment où l'entité collecte des données à caractère personnel sur les salariés (logs de connexion, durée de visite de certains sites...).

Quelles sont les dispositions légales concernant la mise en place d'une solution de filtrage de contenus en entreprise ?

En cas d'infraction et de poursuite, l'entreprise ou l'administration doit s'engager à conserver les logs pour une durée minimale d'un an.

Une non-conservation ou un non-respect de la durée minimale de conservation est puni pénalement d'un an d'emprisonnement et de 75 000 euros d'amende (350 000 euros pour une personne morale).

En réalité les durées de conservation minimale varient :

- La directive européenne prévoit une durée minimale de 6 mois et maximal de 2 ans.
- L'article 6 de la loi pour la confiance dans l'économie numérique prévoit une durée de 1 an.
- La Loi relative à la lutte contre le terrorisme préconise 1 an (loi 2006-64 du 23 janvier 2006).
- La CNIL recommande 6 mois à des fins de contrôle des utilisateurs.

Mais il n'en reste pas moins que la conservation des logs doit être précisé dans la charte informatique, diffusée individuellement et collectivement.

Alt F4 PC

Politique de confidentialité

1. Notre politique de mot de passe

- Chaque mot de passe devra faire au minimum 8 caractères et être composé au minimum d'une majuscule et d'un chiffre.
- Les mots de passe ne doivent pas être des éléments personnels (nom, prénom, date de naissance...)
- Les mots de passe devront être changés au minimum tous les trois mois et ne devront pas être similaire aux précédents.
- Les mots de passe sont strictement personnels et confidentiels, en aucun cas ils ne devront être donnés à des tiers ni présent sur un document servant d'aide-mémoire.

Le service informatique ne demandera jamais les identifiants de connexions d'un utilisateur par e-mail ou par téléphone.

2. Sécurisation de l'accès aux données

Afin de protéger au maximum l'accès aux données sensibles des utilisateurs, nous allons mettre en place un serveur ainsi qu'un contrôleur de domaine qui permettra aux utilisateurs de s'authentifier sur le réseau de l'entreprise. Cette solution va permettre de contrôler les droits de chacun sur les différents dossiers et ressources du réseau, et empêcher ainsi les personnes non autorisées à accéder à celle-ci.

3. Sécurisation de données

Afin de garantir au maximum la sécurité de vos données, nous allons mettre en place plusieurs protocoles de sécurité, tant physique que logiciel.

Tout d'abord au niveau logiciel, nous installerons un logiciel antivirus sur tous les postes informatiques ainsi que sur les serveurs.

Nous mettrons en place des profils utilisateurs au sein de l'entreprise de façon à ce que chaque salarié ou intervenant externe n'ait accès qu'aux applications et aux données dont il a besoin dans le cadre de ses fonctions.

L’accès à un poste informatique sera protégé par un identifiant et un mot de passe qui ne sont connu que par le salarié en question, le service informatique.

Un pare-feu sera inclus, celui-ci aura pour fonction de filtrer le contenu venant de l’extérieur avant qu’il ne pénètre dans le réseau de l’entreprise.

Ensuite au niveau physique, l’ensemble des serveurs et disques de sauvegarde seront stockés dans un local climatisé et fermé à clé, le jeu de clés sera réparti entre les membres du service informatique, l’accès y sera totalement interdit à toutes personnes étrangères au service.
Cette mesure empêchera l’intrusion et l’accès aux données, à des personnes malintentionnées.
Un système de sauvegarde sera mis en place :

- Les sauvegardes journalières et automatisées
- Les supports de sauvegarde seront stockés dans le local Baie sécurisée.
- Le technicien ALTF4PC sera tributaire du bon déroulement des sauvegardes
- Une procédure de rétablissement fonctionnel en cas de dysfonctionnement.

Toujours au niveau physique, aucun poste, serveur ou disque dur ne touchera directement le sol ou les murs afin d’éviter toute détérioration extérieure.

Le local ou la baie de stockage est présenté sera entièrement sécurisé (clé, code d'accès par badge). Le service informatique aura la gestion des accès à cette Baie.

Nous installerons également plusieurs onduleurs sur les serveurs, cette solution va permettre le maintien de l’alimentation électrique en cas de coupure, si la coupure dure trop longtemps, les serveurs recevront l’ordre de s’éteindre « proprement ».

4. Sensibilisation utilisateur

De nos jours, toutes les entreprises sont menacées, quelle que soit leur taille ou leur activité. L'ensemble des utilisateurs sont donc concernés par la sécurité, la connaissance des cyber-risques ne peut plus se cantonner aux personnes du service informatique. Par ailleurs, cette « culture de la sécurité digitale » vous permettra de faire de meilleurs choix en matière de protection. Voici pourquoi nous voulons vous sensibiliser à cela.
Les mesures de sécurité sont essentielles à différents niveaux :

- Elles protègent l'ensemble des biens contre les menaces
- Elles permettent de se tenir en conformité, préservent la réputation de son entreprise
- Elles participent à instaurer une relation de confiance avec l'ensemble des parties prenantes de l'entreprise (client, fournisseurs, salariés, etc.).
- Elles contribuent à la pérennité de l'activité

Les origines des menaces sont diverses et de différentes natures :

- Opérationnel : dysfonctionnement du système à un instant, exemple d'un bug de logiciel
- Physique : accidents naturels ou matériels
- Humaines : erreurs diverses liées aux utilisateurs du matériel informatique

Pour se protéger, il faut répondre à 4 enjeux de sécurité appelé "DICP" :

- **Disponibilité** : sauvegarde sur un support externe ou sur un serveur distant.
- **Confidentialité** : différentes solutions de chiffrement existent pour répondre aux différents besoins : fichiers, dossiers partagés, vol de machines, messagerie ...
- **Intégrité** : utilisation d'outils de hachage tels que Tripwire ou équivalent.
- **Preuve** : utilisation d'outils de signature électronique, tatouage de fichiers (watermarking)

Pour aider à la sensibilisation, nous vous proposons une ou plusieurs interventions sur site ainsi qu'une série de courte vidéo sur différents thèmes liés à la sécurité informatique que

nous pourrons présenter lors de ces passages. Nous mettrons à votre disposition des flyers ainsi que des rappels automatiques pour le changement de mot de passe.

Afin d'informer au mieux les utilisateurs des règles de bon usage de l'outil informatique en entreprise, une charte informatique leur sera adressé par mail, approuvé puis signé par chacun. (Voir charte informatique en annexe)

Continuité des services, support et accompagnement de qualité aux utilisateurs

La continuité de service en cas de panne :

- Un service de Hotline avec prise en main à distance tenu par des techniciens, disponible du lundi au samedi de 9h00 à 18h00.
- Dépannage sur site de J+0 à J+2, en fonction du type de pannes.
- Technicien dédié sur site
- Matériel de Spare

Le relationnel client :

- Être à votre disposition et à votre écoute.
- Respecter la confidentialité et assurer la sécurité des documents et informations confiés.
- Notre personnel intervenant dans votre société doit respecter le règlement intérieur qui la régie.
- Traiter vos réclamations dans les meilleurs délais.

Qualité de prestation :

- Mettre en place une solution adaptée à vos besoins.
- Equipe technique composée de personnel qualifié.
- Sécurité et productivité.
- Respecter les délais

Suivi de l'intervention :

- Suivi interne de l'historique d'appel. Un compte rendu mensuels sera mis à disposition de la Direction d'AutoConcept
- Procédure de suivi qualité des interventions, par un système de fiche rempli par l'utilisateur. (PV de recette d'intervention)

Mesures préventives

- Gestion et mise à jour antiviral du parc informatique
- Sauvegarde et contrôle quotidienne d'une image système local
- Sauvegarde cloud
- Contrôle sauvegarde cloud
- Contrôle espace disque
- Contrôle état des disque durs

- Mise à jour des sécurités Windows

Mesures curatives

- Hotline 5 / 7 Astreinte Week-end avec numéro dédié
- Remplacement matériel J +2heures
- Helpdesk poste de travail
- Restauration des données en cas de panne
- Redémarrage des machines et de applications

Sécurité et productivité du système d'information

Garantir un meilleur accès aux données.

En centralisant les données vous permettez une meilleure synchronisation des informations et un meilleur accès aux fichiers. Cela facilite les échanges ce qui permet d'améliorer la productivité en entreprise. De plus, un accès facile aux données permet à vos collaborateurs nomades de travailler depuis n'importe quel appareil, en toute sécurité.

Disposer d'un système informatique performant.

La performance de votre système informatique est un élément clé de la productivité en entreprise. Il est nécessaire d'optimiser votre système afin d'éviter les processus fastidieux et les tâches inutiles. Vos équipes doivent pouvoir compter sur un matériel informatique performant et rapide, adapté à leur mode de travail et à leurs besoins.

Maîtriser l'accès à internet dans son entreprise.

Contrôler l'accès à internet au sein de votre entreprise empêcher vos collaborateurs d'accéder à certains sites dangereux ou non nécessaires à leur activité comme les sites de téléchargement, les sites de streaming ou les réseaux sociaux. Une maîtrise de l'usage d'internet garantit une meilleure sécurité en limitant l'accès aux sites malveillants et améliore la productivité en entreprise.

Limiter l'impact des pannes informatiques sur la productivité.

Une défaillance du système informatique paralyse votre activité. Il est donc primordial de pouvoir compter sur un prestataire informatique fiable et réactif pour intervenir rapidement, sur site, par téléphone ou par prise en main à distance. Une intervention rapide limite l'impact des pannes informatiques sur la productivité en entreprise.

Former les employés.

Les technologies informatiques évoluent très rapidement et il est important que vos employés puissent maîtriser ces outils afin de gagner en productivité. La mise à niveau des connaissances informatiques de vos collaborateurs peut être effectuée lors de formations dédiées. Un personnel bien formé est la garantie de la pérennité du système d'information en limitant les mauvais usages et les pratiques dangereuses**.**

Anticiper les problèmes informatiques.

La mise en place d'un système de monitoring vous permet de détecter les activités anormales dans votre système d'information ainsi que les tentatives d'intrusion éventuelles.

Le monitoring est donc un moyen d'anticiper les problèmes informatiques et d'agir avant qu'ils ne nuisent sévèrement à votre activité. Le monitoring limite l'impact des pannes et des piratages informatiques sur la productivité en entreprise.

L'infogérance

Faire appel à AltF4 PC vous permet de limiter les conséquences des pannes informatiques sur l'activité de votre entreprise. Nous vous conseillions pour optimiser votre système d'information et garantir la sécurité de vos données. Une informatique maîtrisée représente un gain de temps et d'argent pour votre société et vous permet d'améliorer la productivité en entreprise. Confiez votre informatique à un prestataire qualifié pour disposer d'un système fiable et efficace tout en vous consacrant pleinement à votre cœur de métier.

Alt
F4 PC

CHARTES

Charte de Qualité Service client

Afin de vous satisfaire au mieux, nous nous engageons à :

1. Traçabilité des interventions
    - Chaque intervention est suivie et sauvegardée en interne, cela permet en autres d'identifier et de comprendre plus rapidement les causes de dysfonctionnements
    - Suivi de qualité des interventions par le biais de fiche client (tickets)
    - Nous nous engageons agir avec politesse et respecter votre confidentialité lors des interventions.
2. Continuité de services
    - Services de hotline avec prise en main à distance 24h / 7j ainsi que des interventions maintenues de nuit ou en week-end.
    - Dépannage sur site de J+0 à J+2, en fonction du type de pannes.
    - Réactivité des interventions sur site
    - Mise à disposition de matériel de remplacement
3. Amélioration continue
    - Formation continue de nos techniciens
    - Amélioration permanente des processus de l'entreprise basé sur le P.D.C.A
    - Enquête de satisfaction client à chaque intervention
4. Qualité des prestations
    - Nous vous proposons une solution informatique sur mesure, calqué sur vos besoins et aux meilleurs prix
    - Nous garantissons l'intégrité des licences et logiciels installés

Politique informatique

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

1. Sécuriser l'accès au compte

Le contrôle d'accès logique permet d'identifier toute personne utilisant un ordinateur.

Cette identification permet, à chaque connexion, l'attribution de droits et privilèges propres à chaque utilisateur sur les ressources du système dont il a besoin pour son activité.

Une identification (login + mot de passe) unique est confiée à chaque utilisateur. Ce dernier est personnellement responsable de l'utilisation qui peut en être faite, et ne doit en aucun cas la communiquer.

Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : ..... Un mot de passe doit, pour être efficace, comporter 8 caractères alphanumériques. Il ne doit pas être, notamment, identique au login, même en inversant les caractères, comporter le nom et/ou prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

2. Courrier électronique

Les éléments de fonctionnement de la messagerie à considérer sont les suivants.

Un message envoyé par Internet peut potentiellement être intercepté, même illégalement, et lu par n'importe qui.

En conséquence, aucune information stratégique ne doit circuler de cette manière, sauf à la crypter. *(Précisez si cette possibilité est offerte, si oui dire laquelle et comment, si non dire quel mode de transmission utiliser).*

Il est *(interdit / permis)* d'utiliser des services d'un site web spécialisé dans la messagerie.

Lors du départ d'un collaborateur, il doit être indiqué au responsable de l'administration du système ce qu'il sera fait des fichiers et courriers électroniques de l'utilisateur.

Les messages électroniques sont conservés sur le serveur de messagerie pendant une période de ..... jours et il existe des copies de sauvegarde pendant une période de ..... jour.

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

a. Utilisation privée de la messagerie

L'utilisation du courrier électronique à des fins personnelles est autorisée dans des proportions raisonnables et à la condition de ne pas affecter le trafic normal des messages professionnels.

b. Contrôle de l'usage

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

- Le nombre des messages échangés *(préciser : de façon globale / par service / par utilisateur)*
- La taille des messages échangés ;
- Le format des pièces jointes.

3. Utilisation d'Internet

Chaque utilisateur doit prendre conscience qu'il est dangereux pour l'entreprise :

- De communiquer à des tiers des informations techniques concernant son matériel ;
- De connecter un micro à Internet via un modem *(sauf autorisation spécifique)* ;
- De diffuser des informations sur l'entreprise via des sites Internet ;
- De participer à des forums *(même professionnels)* ;
- De participer à des conversations en ligne (« chat »).
- De télécharger sur des sites

a. Utilisation d'Internet à des fins privées

L'utilisation d'Internet à des fins privées est tolérée dans des limites raisonnables et à condition que la navigation n'entrave pas l'accès professionnel.

b. Contrôles de l'usage

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

- Les durées des connexions *(préciser : de façon globale / par service / par utilisateur)* ;
- Les sites les plus visités *(préciser : de façon globale / par service).*

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

4. Pare-feu

Le *(les)* pare-feu vérifie*(nt)* tout le trafic sortant de l'entreprise, aussi bien local que distant. Il vérifie également le trafic entrant constitué de ..... *(précisez : la messagerie électronique et/ou l'échange de fichiers, et/ou la navigation sur Internet).*

Il détient toutes les traces de l'activité qui transite par lui s'agissant :

- De la navigation sur Internet : sites visités, heures des visites, éléments téléchargés et leur nature (textes, images, vidéos ou logiciels) ;

- Des messages envoyés et reçus : expéditeur, destinataire(s), objet, nature de la pièce jointe *(et éventuellement texte du message).*

Il filtre les URL des sites non autorisés par le principe de la liste noire. Les catégories des sites visés sont les sites diffusant des données de nature pornographique, pédophile, raciste ou incitant à la haine raciale, révisionnisme ou contenant des données jugées comme offensantes *(complétez si nécessaire).*

5. Sauvegardes

La mise en œuvre du système de sécurité *(ne)* comporte *(pas)* des dispositifs de sauvegarde des informations *(et/ou)* un dispositif miroir destiné à doubler le système en cas de défaillance.
Ceci implique, entre autres, que la suppression par un utilisateur d'un fichier de son disque dur n'est pas absolue et qu'il en reste une copie :

- Sur le dispositif de sauvegarde ou miroir ;
- Sur le serveur ;
- Sur le proxy ;
- Sur le firewall (pare-feu) ;
- Chez le fournisseur d'accès.

Ce présent document sera annexé au règlement intérieur. (En annexe)

Il sera diffusé par courrier électronique à l'ensemble du personnel et devra être retourné au service RH. (Paraphe de chaque page, déclaration sur l'honneur et signature).

6. Antivirus

Afin de garantir la sécurisation des postes, AltF4Pc vous recommande d'installer un antivirus sur chacun des postes utilisateurs.

Pourquoi est-il fortement conseillé d'installer un antivirus ?
La principale raison est la protection des données professionnelles et personnelles de AutoConcept.
Les antivirus doivent aujourd'hui être installés sur tout type de support informatique (ordinateurs, smartphones, tablettes...) car les virus informatiques ne se limitent plus qu'aux ordinateurs.
Nous vous proposons BitDefender qui se révèle être le plus avantageux, c'est un antivirus bien réputé dans les entreprises du monde entier pour sa sécurité informatique.

Dispositions légales relatives à la mise en place d'une solution de filtrage de contenus en entreprise

En accord avec la CNIL, d'après l'article L2323-32 du code du travail, 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. Il doit cependant consulter et informer le comité d'entreprise. Les salariés doivent être également informés, notamment de la finalité du dispositif de contrôle et de la durée pendant laquelle les données de connexion sont conservées.

Mail :

L'employeur peut contrôler et limiter l'utilisation d'internet et de la messagerie. Par défaut, les courriels ont un caractère professionnel.
Les limites au contrôle de l'employeur

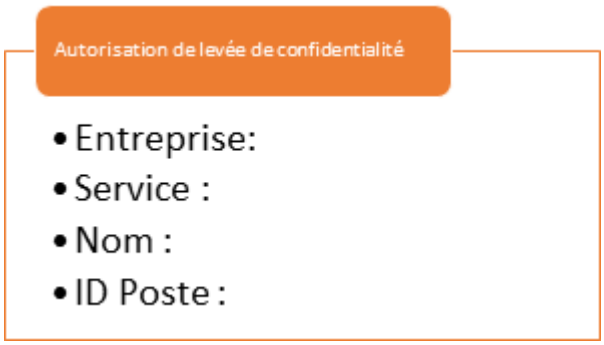
- L'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif,
- Les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite
- Les logs de connexion ne doivent pas être conservés plus de 6 mois.
- La protection des courriels personnels :

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.



<u>Autorisation de levée de confidentialité</u>

Je soussigné Monsieur/Madame ....., exerçant les fonctions de ..... au sein de la société ....., autorise la société ALT F4PC à accéder à mes données personnelles, dans le cadre de l'intervention effectuée sur mon poste dans le but de le restaurer. J'ai bien été informé des risques encourus par cette intervention et, que la société ALT F4PC s'engage dans la mesure du possible à conserver lesdites données, et en aucun cas ne les diffusera.

Fait à ....., le .... / .... / ....

Signature :
(Précédée de la mention « lu et approuvé)

Alt
F4 PC

Mémo

Horaires :
Lundi: 9h-12h ; 14h-18h
Mardi: 9h-12h ; 14h-18h
Mercredi: 9h-12h ; 14h-18h
Jeudi : 9h-12h ; 14h-18h
Vendredi : 9h-12h ; 14h-18h
Samedi : 9h-12h
Tel : 03 87 50 51 52
contact@altf4pc.fr

Une Entreprise à votre image

Courtoisie, souriant, tenue adaptée

Nous comptons sur vous lors de chacun de vos interventions sur site

Alt
F4 PC

Un Monde à votre écoute

www.Altf4maintenance.com

OMEN

So

INFO

Vous êtes l'image de l'entreprise !

1. Vous représentez notre chère société, et la première impression est souvent la bonne ! Il est donc important de soigner l'image que vous reflétez.
2. Il est important d'être courtois, souriant, à l'écoute et pédagogue pour donner le sentiment au client d'être compris.
3. Il est important également d'être ponctuel.

La confidentialité et sécurité avant tout

1. Notre société garantie la sécurité des données, cela passe donc par vous en priorité ! Ne récupérez aucune donnée de nos clients !
2. Le respect et la confiance sont primordiales pour une bonne relation avec nos clients
3. N'oubliez pas de présenter notre clause de confidentialité
4. Toutes transmissions de données à des tiers non concernés sera soumise à sanctions autant sur le plan pénal qu'en interne.

La prestation

1. Des interlocuteurs toujours à l'écoute. Présentez-vous et présentez votre société
2. Garder une trace de vos interactions avec nos clients
3. Sans solutions immédiates à une problématique gardez un contact régulier avec nos clients pour les tenir informés des avancées.
4. Tout problème a sa solution, si toi tu ignores la solution ton collègue se fera un plaisir de t'aider

GLOSSAIRE

GLPI : c'est un outil de gestion de parc informatique fonctionnant avec le principe des tickets. Il est libre et gratuit.

Contrôleur de domaine : Les contrôleurs de domaine stockent les données et gèrent les interactions entre l'utilisateur et le domaine, y compris les processus d'ouverture de session, l'authentification et les recherches dans l'annuaire.

Pare feu : est un logiciel et/ou un matériel, permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communication autorisés sur ce réseau informatique. Il mesure la prévention des applications et des paquets.

Serveur data : Un serveur data est un serveur ayant pour rôle de stocker les données et d'en faire des sauvegardes.

Serveur applicatif : un serveur d'application est un serveur servant à exécuter des logiciels directement sur celui-ci plutôt que le poste de l'utilisateur, qui devient alors un client léger.

Routeur : Un routeur est un équipement d'interconnexion de réseaux informatiques permettant d'assurer le routage des paquets entre deux réseaux ou plus afin de déterminer le chemin qu'un paquet de données va emprunter.

Paquets : Un paquet inclut un en-tête (en anglais, header), comprenant les informations nécessaires pour acheminer et reconstituer le message, encapsule une partie des données.

Switch : Un switch désigne un commutateur réseau, équipement ou appareil qui permet l'interconnexion d'appareils communicants, terminaux, ordinateurs, serveurs, périphériques reliés à un même réseau physique.

Annexe

Charte informatique

La présente charte est applicable à compter du 09/12/2020.
Elle a été adoptée après consultation du comité d'entreprise en date du 10/11/2020 par la société AutoConcept et le service informatique.
L'entreprise AutoConcept met en œuvre un système d'information et de communication nécessaire à son activité, comprenant notamment un réseau informatique et téléphonique important.
Les salariés, dans l'exercice de leurs fonctions, sont amenés à utiliser les outils informatiques et téléphoniques mis à leur disposition et à accéder aux services de communication de l'entreprise.
L'utilisation du système 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 du système d'information et de communication, la présente charte pose les règles relatives à l'utilisation de ces ressources, Elle définit aussi les moyens de contrôle et de surveillance de cette utilisation mise en place, non seulement pour la bonne exécution du contrat de travail des salariés, mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur.
Elle dispose d'un aspect réglementaire et est annexée au règlement intérieur de l'entreprise.
Elle ne remplace en aucun cas les lois en vigueur que chacun est censé avoir pris connaissance.

Champ d'Application

Cette charte s'applique à l'ensemble des utilisateurs du système d'information et de communication d'AutoConcept, quel que soit leurs statuts, y compris salariés, intérimaires, stagiaires, employés de sociétés prestataires et visiteurs occasionnels. Elle sera annexée aux contrats de prestations.

Les salariés veillent à faire accepter valablement les règles posées dans la présente charte à toute personne à laquelle ils permettraient d'accéder au système d'information et de communication.

Pour des raisons de sécurité du réseau, est également considéré comme faisant partie du système d'information et de communication le matériel personnel des salariés connecté au réseau de l'entreprise, ou contenant des informations à caractère professionnel concernant l'entreprise.

La présente charte ne préjuge pas des accords particuliers pouvant porter sur l'utilisation du système d'information et de communication par les institutions représentatives, l'organisation d'élection par voie électronique ou la mise en télétravail de salariés.

Confidentialité

L'accès à certains éléments du système d'information (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines application ou services interactifs) est protégé par des paramètres de connexion (identifiant, mot de passe).

Dans la mesure du possible, ces paramètres doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit. En tout état de cause, ils ne doivent pas être transmis à des tiers ou aisément accessibles. Ils doivent être saisi par l'utilisateur à chaque accès et ne pas être conservés en mémoire dans le système d'information.

Chaque utilisateur est responsable pour ce qui le concerne du 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 Monsieur Thierry AMET et applicables quel que soit le support de communication utilisé.

L'utilisateur doit être particulièrement vigilant sur le risque de divulgation de ces informations dans le cadre d'utilisation d'outils informatiques, personnels ou appartenant à l'entreprise, dans des lieux autres que ceux de l'entreprise.

Sécurité

Le service informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information et de communication. Elle doit prévoir un plan de sécurité et de continuité du service, en particulier en cas de défaut matériel. Elle veille à l'application des règles de la présente charte. Elle est assujettie à une obligation de confidentialité sur les informations qu'elle est amenée à connaître.

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection desdites ressources, en faisant preuve de prudence et de vigilance. En particulier, il doit signaler au service informatique toute violation ou tentative de violation de l'intégrité de ces ressources, et, de manière générale tout dysfonctionnement, incident ou anomalie.

Internet

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à internet. Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée. En particulier, l'utilisation de l'internet à des fins commerciales personnelles en vue de réaliser des gains financiers ou de soutenir des activités lucratives est strictement interdite.

Bien sûr, il est interdit de se connecter à des sites internet dont le contenu est contraire à l'ordre public, 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.

Messagerie électronique

Chaque salarié dispose, pour l'exercice de son activité professionnel, d'une adresse de messagerie électronique normalisée attribuée par le service informatique. La messagerie est accessible aussi bien à partir d'un navigateur internet grâce à un Webmail.

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 dysfonctionnements qu'ils constatent dans ce dispositif de filtrage. Toute utilisation personnelle de la boite mail ce doit d'être précisé pour éviter toute vérification aux seins de l'entreprise. (Ex : dossier « perso »)

Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ...

Usage personnel des ressources internet

L'accès aux réseaux sociaux et sites non professionnel est interdit pendant les heures de travail.

Information et Sanction

La présente charte est affichée publiquement en annexe du règlement intérieur. Elle est communiquée individuellement à chaque salarié par voie électronique.

Le service informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation du système d'information, en particulier sur la procédure 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 sa sécurité.

Chaque utilisateur doit se conformer aux procédures et règles de sécurité édictées par le service 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 mesure de sécurité 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 donnera également lieu à remboursement de la part de l'utilisateur concerné.

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

- Loi n° 78-17 du 6 janvier 1978 dite « Informatique et Libertés ».

- Tout utilisateur qui contreviendrait aux règles aux règles précédemment définies peut s'exposer à des poursuites civiles et/ou pénales prévues par les textes en vigueur (articles sur la fraude informatique de 323-1 à 323-7 du code pénal).

Cette charte fera l'objet d'une déclaration à la CNIL.
Un système de collecte de données sera mis en place. Les informations recueillies sur ce formulaire sont enregistrées dans un fichier informatique.

<u>Disposition légale pour la solution de filtrage</u>
La solution de filtrage est autorisée à condition qu'elle soit signalée aux employés avant d'être mis en place et qu'ils en connaissent sa portée. Elle doit aussi être déclarée à la CNIL. La loi demande que les logs soient gardés pour une durée de 12 mois maximum.

Tout activité sortant du réseau, navigation sur internet est filtrée et enregistrée sous forme de logs, comme la loi nous y autorise si la collecte est non nominative et/ou que l'entreprise possède un Correspondant Informatique et Liberté. L'information qu'un tel système existe n'est pas forcément obligatoire, mais dans le cas contraire, il doit être déclaré à la CNIL et aux employés.

L'employeur se doit de respecter le secret des correspondances qu'elles soient émises ou reçues par un employé, et qui 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. Les sanctions sont de 1 an d'emprisonnement et de 45 000 € d'amende.

Les droits des employés :

- De demander des informations sur le traitement de vos données à caractère personnel ;
- D'obtenir l'accès aux données à caractère personnel détenues à votre sujet ;
- De demander que les données à caractère personnel incorrectes, inexactes ou incomplètes soient corrigées ;
- De demander que les données à caractère personnel soient effacées lorsqu'elles ne sont plus nécessaires ou si leur traitement est illicite ;
- De vous opposer au traitement de vos données à caractère personnel à des fins de prospection ou pour des raisons liées à votre situation particulière ;
- De demander la limitation du traitement de vos données à caractère personnel dans des cas précis ;
- De récupérer vos données personnelles, dans un format utilisé et lisible par machine, pour un usage personnel ou pour les transférer à un autre organisme ;
- De demander que les décisions fondées sur un traitement automatisé qui vous concernent ou vous affectent de manière significative et fondées sur vos données à caractère personnel soient prises par des personnes physiques et non uniquement par des ordinateurs. Dans ce cas, vous avez également le droit d'exprimer votre avis et de contester lesdites décisions ;
- En cas de dommage matériel ou moral lié à la violation du RGPD, vous disposez d'un droit de recours. Vous pouvez déposer une réclamation auprès de la Commission nationale Informatique et libertés (CNIL) ou introduire une action collective en faisant notamment appel aux associations nationales agréées de défense des consommateurs.

Les entreprises ont l'obligation :

- De respecter le principe de protection des données personnelles et de la vie privée imposées par le règlement, dès la conception de tout projet ;
- De recenser les traitements qu'elles mettent en œuvre dans un registre des traitements ;
- D'être en capacité de prouver que les traitements de données à caractère personnel mis en œuvre respectent les règles applicables, notamment via l'adhésion à des codes de conduite et l'obtention d'une certification ;
- De notifier toute violation de données à caractère personnel par le responsable de traitement et le sous-traitant aux autorités et aux personnes concernées ;
- De réaliser une étude d'impact sur la vie privée pour les traitements à risque ;
- De désigner un délégué à la protection des données pour les organismes publics et les entreprises dont l'activité principale les amène à réaliser un suivi régulier et systématique des personnes à grande échelle ou encore des organismes qui traitent des données dites « sensibles » ou relatives à des condamnations pénales et infractions ;
- De s'assurer que les personnes sont informées, de manière claire et concise, de la durée de conservation des données, de l'existence de profilage, de leurs droits et des voies de recours disponibles ;
- De permettre aux personnes dont les données sont traitées d'exercer leurs droits (à l'oubli, à la portabilité des données, de limitation... etc.).

Charte informatique et de confidentialité

(Conformément à la loi « informatique et libertés » du 6 janvier 1978 modifiée en 2004, vous bénéficiez d'un droit d'accès et de rectification aux informations qui vous concernent, que vous pouvez exercer en vous adressant au service informatique)

Je soussigné Monsieur/Madame ....., exerçant les fonctions de .....

Au sein de la société AUTOCONCEPT, étant à ce titre amené à accéder à des données à caractère professionnel, déclare reconnaître la confidentialité desdites données.

Je m'engage par conséquent, conformément aux articles 34 et 35 de la loi du 6 Janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés, à prendre toutes précautions conformes aux usages et dans le cadre de mes attributions afin de protéger la confidentialité des informations auxquelles j'ai accès, et en particulier d'empêcher qu'elles soient modifiées, endommagées ou communiquées à des personnes non expressément autorisées à recevoir ces informations.

Je m'engage en particulier à :

- Ne pas utiliser les données auxquelles j'ai accès à des fins autres que celles prévues par mes attributions,
- Ne divulguer ces données qu'aux personnes dûment autorisées,
- Ne faire aucune copie des données, non autorisées par mes supérieurs et/ou le service informatique,
- Prendre toutes précautions conformes aux usages afin d'éviter l'utilisation détournées ou frauduleuses
- Des données dont je suis responsable, par une tierce personne non autorisée,

- Prendre toutes mesures conformes aux usages afin de préserver la sécurité matérielle de ces données,
- En cas de cessation de mes fonctions, restituer intégralement les données, fichiers informatiques et tout

Support d'information relatif à ces données.

Cet engagement de confidentialité, en vigueur pendant toute la durée de mes fonctions, demeurera
Effectif, sans limitation de durée après la cessation de mes fonctions, dès lors que cet engagement
Concerne l'utilisation et la communication de données à caractère personnel.
J'ai été informé que toute violation du présent engagement m'expose notamment à des actions et
Sanctions disciplinaires et pénales conformément aux dispositions légales en vigueur.
Fait à ..... le .../ .../....
Signature de l'utilisateur :
(Précédée de la mention « lu et approuvé »