

**Projet SAS**

10/12/2018

*Sommaire :*

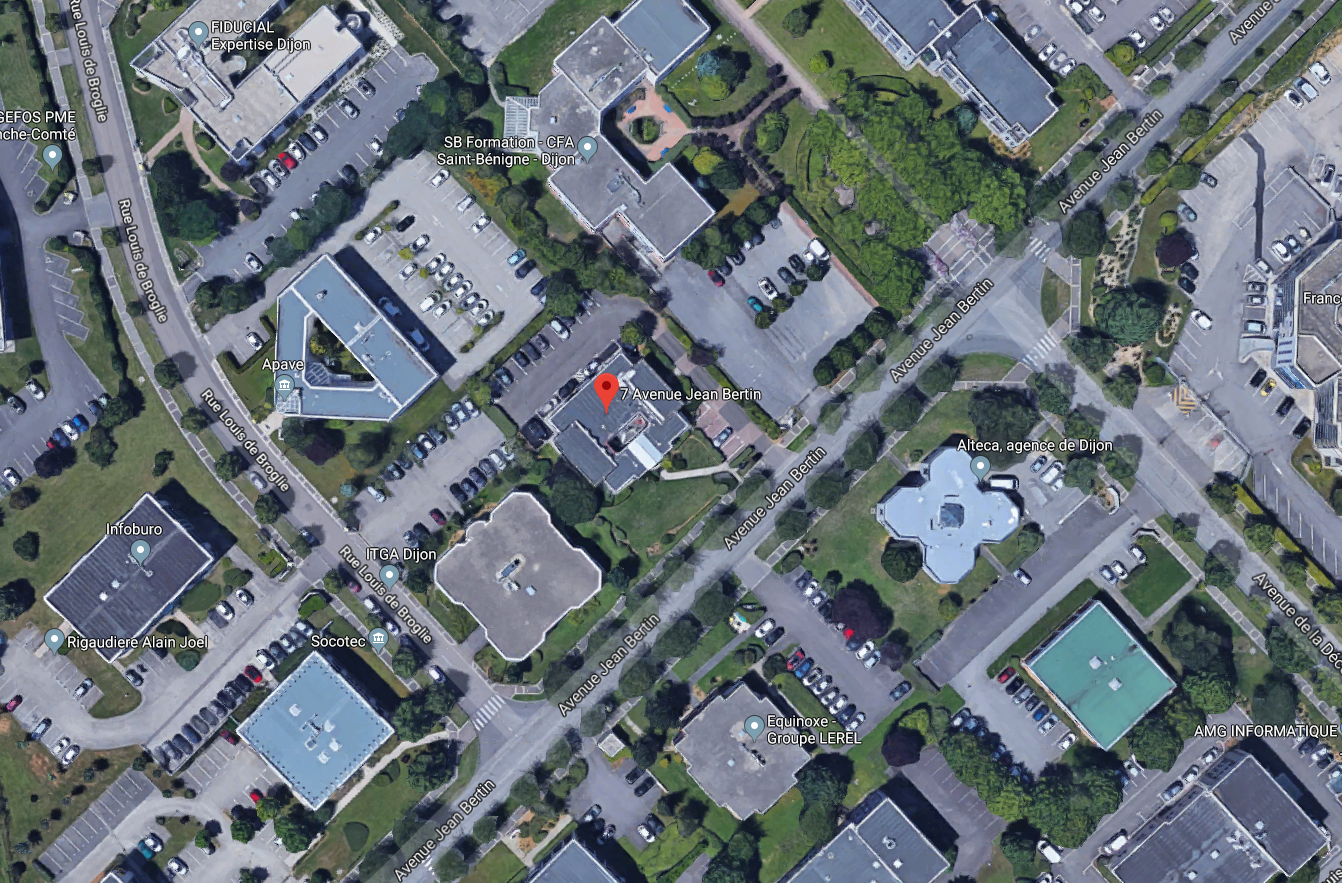
1. *L’entreprise*
2. *Présentation de l’entreprise*
3. *Information complémentaire*
4. *Organigramme*
5. *Etude de l’existant*
6. *Organigramme*
7. *Problématique général*
8. *Problématique technique*
9. *La loi informatique au sein de l’entreprise*
   * 1. *La CNIL*
     2. *Collecter des données personnelles*
     3. *Le rôle de l’entreprise est d’assurer la confidentialité*
10. Mise en place de solutions de contrôle
    * 1. Le droit de filtrer
      2. Installer une solution de filtrage
11. *Plan de sécurisation des données*
    * 1. *La mise en place des bonnes pratiques*
      2. *Ce que nous pourrions apporter à l’entreprise*
      3. *Continuité des services en cas d’incident*
      4. *La mise en place des bonnes pratiques*
      5. *Les comportements à travailler*
      6. *Conclusion*
12. *Charte Qualité AutoConcept*
13. *La qualité de services en cas de panne*
14. *Le relationnel client*
15. *La sécurité et la productivité*
16. *Bonne conduite envers un client*
17. *Proposition de mémo interne*
18. *Conclusion*
19. *Annexes*

# L’entreprise

## Présentation de l’entreprise

Whitechpro est une jeune entreprise spécialisée dans la prestation informatique pour les TPE/PME. Nous pratiquons des audits, la gestion de parc informatique, donnons des conseils et des guides aux utilisateurs. Nous sommes basés dans la zone Valmy de l’agglomération Dijonnaise avec comme ambition de se développer dans toute la région. Notre équipe de 12 techniciens support, 7 techniciens réseaux et systèmes s’occupent d’un portefeuille d’une trentaine de clients. Notre service qualité réalise régulièrement des tests de satisfactions auprès de nos collaborateurs.

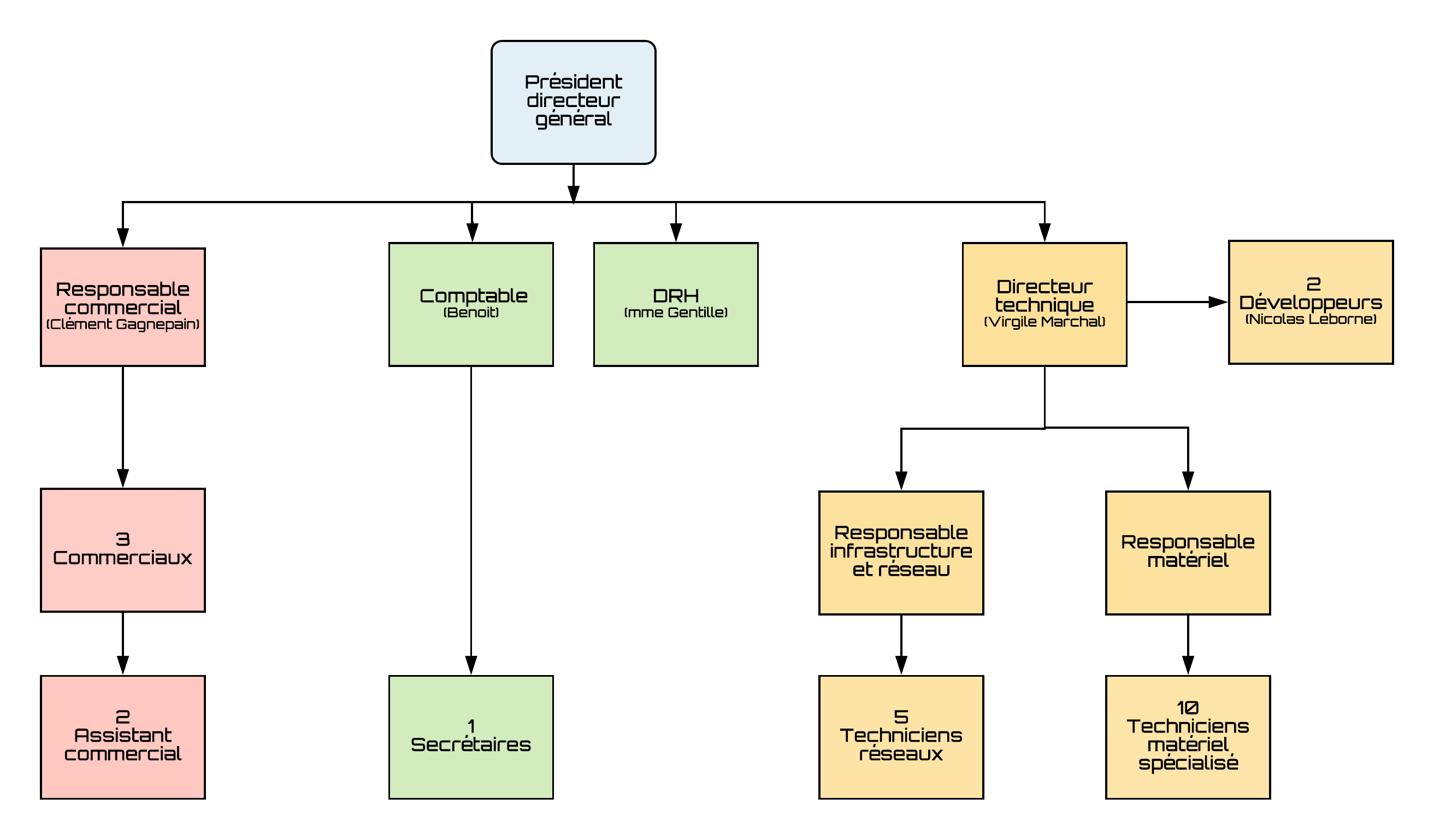
## Information complémentaire



* Date de création : 2008
* Chiffre D’affaire : 2 Millions €
* Statue Juridique : PME
* Siret : 825 045 297 00325
* Adresse : 7 Avenue Jean Bertin
* Clientèles principales : TPE PME



## Organigramme

**

# Présentation AutoConcept

L’entreprise AutoConcept est une société spécialisée dans la vente de véhicules neufs ou d’occasions rassemblant 83 salariés, elle est située route des grand Crue à Dijon. Cette entreprise possède un parc informatique composé de 80 ordinateurs et de plus de 650 véhicules.

AutoConcept fait donc appel à nous dans le but d’externaliser son service informatique et de palier aux différents problèmes informatiques leurs causant d’importantes pertes financières (140 000 €). Suite à cela, si nous obtenons la gestion du parc informatique, nous embaucherons un ancien informaticien de chez vous, que nous accueillerons et que nous accompagnerons. Les prestations informatiques actuelles, sont exécutées par deux informaticiens en interne.



## Organigramme de la société AutoConcept



## Problématiques générales relevées chez AutoConcept

* Nécessité d’augmenter la sécurité dans un milieu professionnel auprès des utilisateurs, notamment par rapport aux mots de passe, à l’intrusion sur les postes, ainsi qu’aux filtrages des connexions
* Manque de sérieux du service informatique qui cause des problèmes de communication du service avec les autres usagers.
* Le renouvellement du matériel est impossible pendant 3 ans.
* Gestion des incidents incorrects qui freine la productivité de l’entreprise et entraine des conditions de travail déplorables.

## Problématiques techniques relevées chez AutoConcept

* « Lenteur de certains postes » 🡪 Nettoyage de disque et optimisation du système d’exploitation, Sinon changement de HDD à SSD.
* « Crash disque du poste d’un commercial » 🡪 Mise en place d’un cloud avec sauvegardes automatiques des disques de nombreuse fois par jour, pour chaque service.
* « Intrusion d’un client sur un poste sans mot de passe » 🡪Mise en place d’une fonction de déconnexion de session au bout de 15 min, puis choisir le procédé pour rendre les mots de place plus complet
* « Version de Windows pirate » 🡪 Achat de licences Windows, à un prix très intéressant grâce à notre collaboration avec Microsoft.
* « Manque d’explication et langage trop technique » 🡪 Explication auprès des usagers à simplifier et rapport écrit clair avec glossaire.

# artcile 2Les données personnelles dans l’entreprise



# 3.A La CNIL

La Commission Nationale de l’Informatique et des Libertés est une autorité administrative indépendante française crée en 1978.Elle exerce ses missions conformément à la loi informatique et libertés. Son principal but est de permettre la protection de la vie privée et des libertés dans le monde du numérique, elle se doit d’anticiper les développements technologiques et de prévoir leurs futures conséquences mais aussi d’informer les personnes concernées par la loi informatique de leurs droits et devoirs. La CNIL a pour mission d’aider les citoyens mais peu aussi infliger des sanctions financières au responsable de traitement de données à caractère personnel n’ayant pas respecté la loi informatique et libertés. Ces sanctions peuvent aller d’un montant maximal de 150 000€, pouvant aller jusqu’à 300 000€ en cas de récidive.

La CNIL est donc l’autorité du monde numérique et est donc garant de notre vie privée et de nos libertés.

## 3.B Collecter des données personnelles

De nos jours, l’entreprise est de plus en plus confrontée à la collecte des données par le biais de matériel informatique, dans la mesure ou ces informations peuvent porter atteintes au droits et liberté des personnes, il faut veiller au respect des règles de protection des données à caractère personnel.

On retrouve 5 principes en cas de collecte, de traitement ou de conservation de données :

* La finalité du traitement
* La proportionnalité et la pertinence des données collectés
* La durée de conservation des données
* La sécurité et la confidentialité des données
* Le respect des droits des personnes

Il est nécessaire de déclarer en ligne ou par courrier à la CNIL tout fichier ou traitements automatisé avant sa création sous peine de sanction pouvant mener à une amende, un avertissement ou l’obligation d’arrêter le traitement des données.

Dans certain cas il n’y a pas lieu d’accomplir cette déclaration :

* Les traitements ayant pour seul objet la tenue d’un registre qui est destiné exclusivement à l’information du public.
* Les fichiers associatifs
* En cas de désignation d’un correspondant a la protection des données
* Les données dont la finalité est d’assurer la conservation a long terme de documents d’archive

## 

## 3.C Le rôle de l’entreprise est d’assurer la confidentialité

Tout salarié peut être le détenteur d’informations sensibles concernant son employeur, la confidentialité des données est indispensable et constitue un point capital pour l’entreprise. Il est excessif de considérer que toute information détenue par le salarié présente un caractère confidentiel, il est important de définir quel type d’information l’est. (Information liés à la clientèle, données relatives au savoir-faire ou procédés technologique).

L’entreprise se doit en tant que responsable du traitement mettre en œuvre la sécurité des locaux et des systèmes d’informations, l’accès aux données est réservé aux personnes désigner et fixer une durée de conservation des fichiers.

Dans le monde de l’entreprise l’obligation de confidentialité se rattache à l’obligation d’exécution du contrat de travail qui a pour particularité de s’exercer pendant mais aussi après à sa rupture.

La jurisprudence est très utilisée dans les cas de la protection des intérêts de l’entreprise, il est possible d’interdire à un ancien salarié, après la fin de son contrat d’écrire sur internet des informations qu’il avait obtenues dans l’exécution de son travail.

Il faut donc agir pour protéger le patrimoine immatériel en établissant une politique globale en sensibilisant et informant le personnel (charte informatique en annexe du règlement intérieur) en organisant une réunion d’information afin trouver un accord sur les conditions d'utilisation du web dans l'entreprise. Les salarié auteurs d’utilisation frauduleuse de donnée seront autant plus fautif et peut-être sanctionné d’une faute grave voir lourde si l’intention était de nuire à l’entreprise. Mais il est impensable que l’employeur se contente de simple soupçon.

# Mise en place de solutions de contrôle.

4.A  *Le droit de filtrer*

Le filtrage a pour but de conditionner l’environnement de travail selon des règles grâce à des logiciels. Ces logiciels permettent entre autres de gérer les connexions au réseau internet de l’entreprise mais aussi l’utilisation du poste des salariés dans l’entreprise

L’arrêté du 27 juin 1989 « le filtrage est la mise en correspondance de formes selon un ensemble prédéfini de règles ou de critères »

Le décret n°2010-1630 du 23 décembre 2010 relatif à la procédure d'évaluation et de labellisation des moyens de sécurisation destinés à prévenir l'utilisation illicite de l'accès à un service de communication au public en ligne.

Les fournisseurs d’accès ont pour devoir d’utiliser le filtrage selon l’Art.227-23

:« la procédure permettant d'empêcher l'accès des internautes aux sites incitant à la commission d'actes de terrorisme ou en faisant l'apologie et aux sites diffusant des images et représentations de mineurs à caractère pornographique. »

Dans son guide pratique pour les employeurs et les salariés, la CNIL considère que s’il n’est pas possible d’interdire de manière générale l’utilisation d’Internet à des fins non professionnelles, en vue du contexte jurisprudentiel actuel rien n’empêche l’employeur de limiter l’accès de ses employés à internet à CNIL reconnaît la possibilité de mettre en place des dispositifs de filtrage de sites non autorisés : sites à caractère pédophile, révisionniste, raciste…

Pour mettre en place un système de filtrage chaque employeur doit informer :

* Des finalités poursuivies
* Des destinataires des données
* De ses droits d’accès et de rectification (connaitre les données qu’un organisme détient sur vous)

L’utilisation des keyloggers (logiciel permettant de tracer tous les caractères saisis sur un clavier par un utilisateur) est encadré par la CNIL, elle considère ce dispositif comme attente excessive a la vie privée des salariés

*4.B Mise en place du filtrage internet*

En régulant l’accès à internet on améliore le fonctionnement de l’entreprise avec une utilisation plus professionnelle d’internet et donc un gain de productivité, cela permet de réduire les risques d’attaques du réseau informatique (réseau) mais aussi d’avoir une connexion à internet plus fluide.

Il y a deux types de régulation d’accès à internet : en limitant le temps et en filtrant le contenu, il est possible d’utiliser les deux simultanément.

Afin de limiter le temps d’utilisation d’internet on retrouve une solution amiable, définir une limite quotidienne ou hebdomadaire avec vos salariés, mais il est préférable d’envisager l’utilisation de logiciel (Elimit) et de le déployer sur chaque PC en réseau.

Le plus intéressant est de filtrer le contenu consulté par les utilisateurs, cette méthode doit être confier à l’administrateur réseau.

On retrouve 3 types de filtres, il est possible de définir des mots clés interdits d’utilisation et donc l’utilisateur ne peut accéder au résultat dans un moteur de recherche, de bannir des Url prédéfini comme des sites de vidéos en ligne ou de jeux, mais aussi de filtrer le téléchargement de certain fichier (vidéo, musique) et ainsi limiter le risque de virus.Bas du formulaire

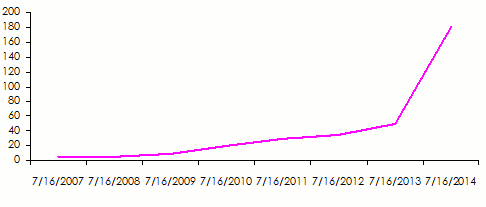
# Plan de sécurisation des données

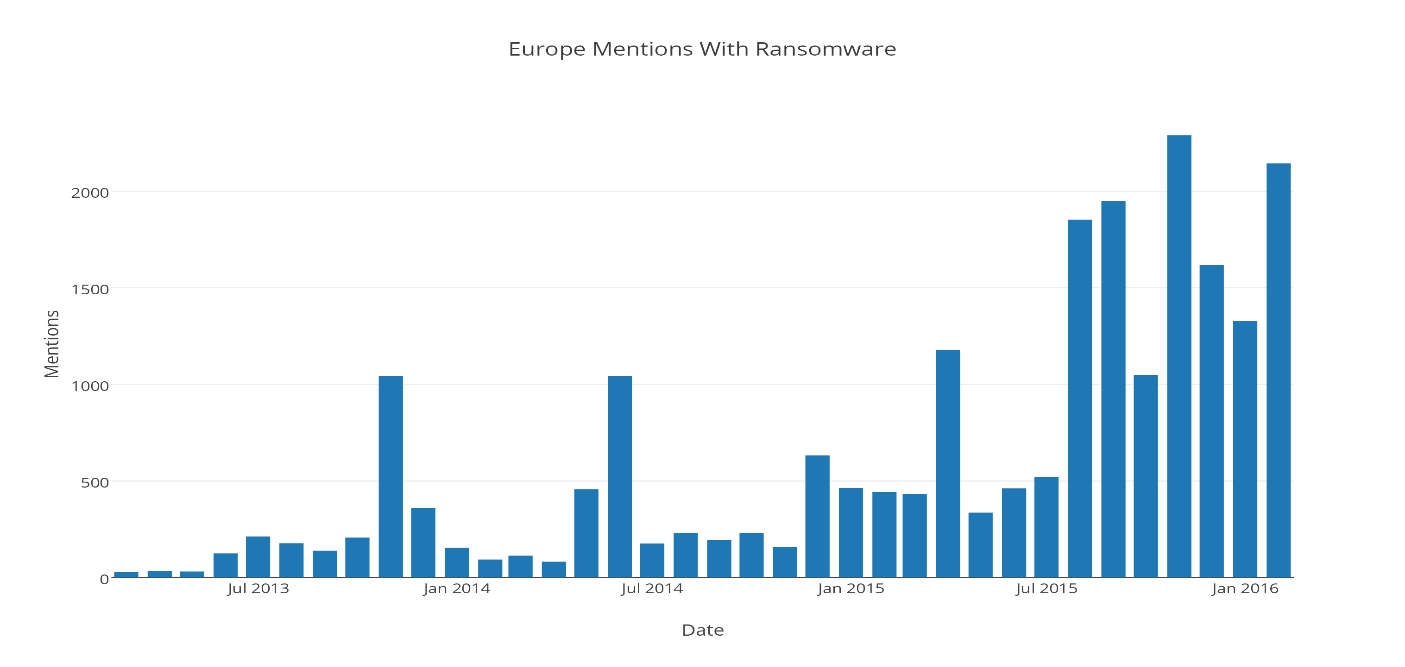
## 5.A Présentation

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Tableau analyse du risque** | | | | | | |
| Identification | Probabilité  (1 à 4) | Impact  (1 à 4) | Criticité | Solution | Nouvelle Criticité | Estimation de la réduction du risque |
| Piratage poste | 3 | 4 | 12 | Utilisé des mots de passe complexe et d’antivirus puissant | 4 | 66% |
| Crash disque | 3 | 4 | 12 | Sauvegarder les données au préalable, puis remettre les données sur un nouveau disque | 4 | 66% |
| Délais d’intervention | 4 | 4 | 16 | Disposer des pc de prêt | 4 | 75% |
| Intrusion dans la salle des serveurs | 2 | 4 | 8 | Externaliser les données | 4 | 50% |
| Fuite de données faite par un salarié de l’entreprise | 2 | 4 | 5 | Mettre en place un système de journal de tout ce qui transite sur le réseau de l’entreprise, et ne pas autoriser l’exportation de fichiers sur une clé USB | 4 | 50% |
| Inondation/ coupure d’électricité entraînant la destruction des serveurs | 3 | 4 | 12 | Mettre en place un groupe électrogène sur les serveurs à l’étage. Ou externaliser les serveurs | 4 | 66% |
| Tempête électromagnétique du Soleil | 3 | 4 | 12 | Mise en place d’une cage de Faraday sur les serveurs, et coupure de toutes les alimentations (pc, écrans, frigos etc..) | 4 | 66% |

La cybersécurité est devenue un élément essentiel dans la vie de l’entreprise, en effet, le nombre d’attaque, et la façon dont les entreprises sont attaquées ont évolué. Comme le montre ces graphiques :

**Nombre de cas de piraterie recensés dans le monde par jour entre 2007 et 2014**

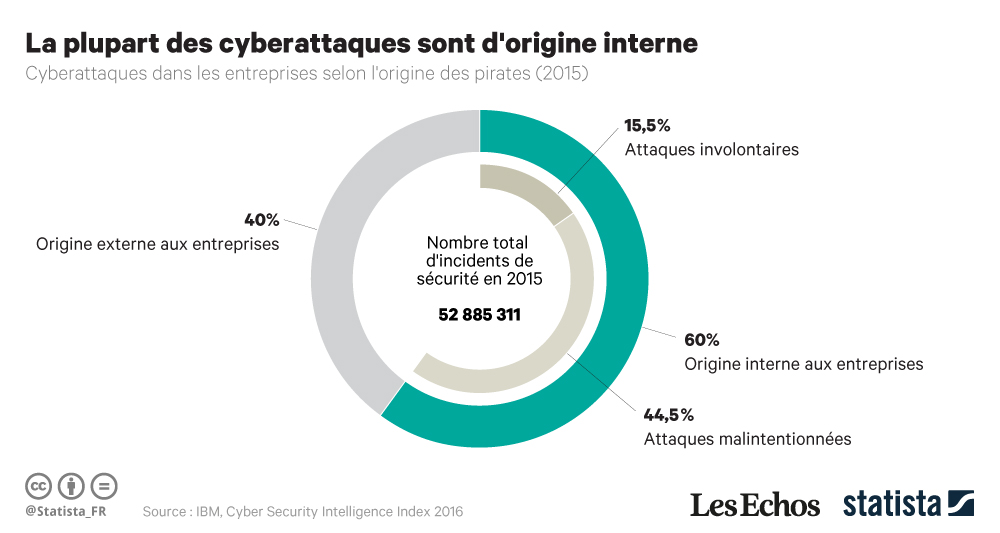
 Nous pouvons voir sur ce graphique que le nombre de cyber attaques est en constante augmentation. On estime qu’en 2013, 42 800 000 événements de ce type ont eu lieu, soit plus de 117 000 par jour. Tout en continuant d’avoir une évolution exponentielle, le nombre d’événements passe alors à 180 000 par jour courant 2014. Cette augmentation est causée par l’appât du gain, et par l’envie de se faire de l’argent facile.

**Nombre de cas de piraterie amenant à une demande de rançon en Europe **

Nous pouvons donc aisément affirmer que pour les années suivants 2014 et 2016, le nombre d’attaque et les façons de pirater, stagnent, ou sont en augmentation. Ces graphiques nous permettent de remarquer que la dangerosité et la fréquence de ces attaques sont très importantes, et le deviennent de plus en plus.

A contrario sur le prochain graphique nous allons voir que dans 60% des cas, l’attaque vient de l’intérieur de l’entreprise.

**Répartition des origines de cyberattaques dans les entreprises**



Ce graphique met en valeur l’importance d’avoir des personnes spécialisées en informatique car il n’y a pas « qu’une seule porte à boucher ».

« Selon le gouvernement britannique, il s’écoule, en moyenne, 200 jours entre l’installation d’un logiciel malveillant et sa détection. Ce nombre est de 173,5 jours selon PricewaterhouseCoopers (PwC). »

Ce nombre impressionnant reflète un réel manque d’expert en sécurité informatique dans les entreprises. En effet la simple mise en place d’antivirus ne suffit pas, dans le monde de l’intrusion informatique, les pirates ont toujours de l’avance sur les technologies ou les programmes actuels. Une connaissance accrue et perpétuelle dans ce milieu est le seul moyen de s’assurer une sécurité sur le long terme. Que ce soit au niveau de la mise en place des bonnes pratiques, ou côté « logiciel ».)

## 5.B Ce que nous pourrions mettre en place dans l’entreprise

Messages intempestifs de « version de Windows pirates »

Toutes nos licences sont certifiées, notre collaboration avec Microsoft, CISCO et HP, en autre, nous permet d’être certain de l’authenticité des produits et des licences. Tout en restant à des prix très compétitifs en toute légalité. Toute utilisation de copie pirate est très sévèrement punie par la loi, et la sanction est multipliable selon le nombre de poste concernés.



[Cette photo](http://wccftech.com/windows-10-technical-preview-update-coming/) par Auteur inconnu est soumis à la licence [CC BY-SA-NC](https://creativecommons.org/licenses/by-nc-sa/3.0/)

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

Une image contenant objet

Description générée automatiquementCeci est une des multiples facettes de la sécurité informatique, en effet bloquer l’accès à certains noms de domaine, ou certains sites, peut empêcher les employés d’entrer des informations sensibles (identifiant, mail, mot de passe etc..) sur des sites pirates reprenant votre page de connexion par exemple. Cela permet également d’éviter que les malfrats envoient des mails malicieux, ou fassent toutes autres opérations qui peut les aider dans leurs quêtes de vols, de destructions et de rançons. La sécurité informatique passe également par le fait de saisir les identifiants uniquement via les sites officiels. Ils sont la plupart du temps reconnu par leur barre en « https », et avec un cadenas comme ceci :

Tout de même, le mieux serait de retenir au fur et à mesure du temps l’adresse exacte. Car le cadenas et le « https » sont très facile à avoir et ne garantissent pas un site officiel, cela donne juste une bonne information dans un premier temps. Cette technique, permettra aux employés de s’assurer de la véracité des informations, et des sites avec le temps.

Cependant, la mise en place de ce système de filtrage implique des contraintes, assez récemment, avec le vote de la loi RGPD ; toute entreprise doit obligatoirement pouvoir donner des informations précises, sur le site auquel la personne a essayé, ou s’est connectée.



[Cette photo](https://www.internautas.org/) par Auteur inconnu est soumis à la licence [CC BY](https://creativecommons.org/licenses/by/3.0/)

Nous pouvons citer par exemple l’adresse informatique de l’ordinateur en question, l’heure de la connexion, l’identité de la personne qui s’est connectée (d’où l’importance de restreindre l’accès de son ordinateur, entre-autre). L’entreprise devra également donner le contenu qui a été rentré dans la page. Ce manquement au règlement, pourra impliquer la responsabilité du directeur de l’entreprise, notamment lors d’une enquête de la police.

Ce que nous pouvons mettre en place n’est pas obligatoirement présent « dans » l’ordinateur, en effet l’installation ou la maintenance préventive de certains équipements sont souvent négligés dans les entreprises. Le branchement d’un onduleur, ou d’un groupe électrogène sont des solutions efficaces lors d’une coupure de courant ou d’un court-circuit par exemple. Avec une possibilité de positionner ces installations à un étage, nous pourrions alors écarter le danger qu’implique une inondation.

Nous pouvons également mettre en place des solutions de prévention sur vos équipements, un dépoussiérage, un nettoyage des disques, ou bien maintenir les logiciels à jour. Cela permet de diminuer les risques d’une panne un d’un dysfonctionnement « logiciel » grave, entrainant un dysfonctionnement qui peut s’avérer critique ou très gênant.

Il est également fortement recommandé de placer à minima une alarme, voir des caméras pour être averti lors de la venue de cambrioleurs. Cela permettra de pouvoir donner des éléments d’enquêtes aux forces de l’ordre, et des preuves pour l’assurance. Nous ne pouvons pas écarter l’hypothèse d’un salarié voulant compromettre des données, pour cela, un système de badge à l’entrée de la salle des serveurs et une porte en aluminium pourraient parfaitement faire l’affaire. Sinon, nous pouvons prendre en charge toutes vos données sur nos serveurs, cela vous permettra de vous assurer un service irréprochable et infaillible.



[Cette photo](https://fr.wikipedia.org/wiki/Onduleur) par Auteur inconnu est soumis à la licence [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)

## 5.C Continuité des services en cas d’incident

Voici une de vos problématiques : « Crash disque du poste d’un commercial : perte d’exploitation 80000 euros. »



[Cette photo](http://info.sio2.be/kpz/1/11.php) par Auteur inconnu est soumis à la licence [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)

Pour pallier ce problème, nous procéderions à des sauvegardes en instantané à plusieurs endroits sécurisés, afin de toujours pouvoir garantir leurs authenticités et leurs sécurités, nous mettrons bien entendu en parallèle un système plus poussé de dossier partagé avec des restrictions selon la personne qui souhaite accéder à la ressource. Les données présentent sur ces machines seront bien évidemment disponibles à n’importe quel moment, et un système de sauvegarde automatique permettra de récupérer des données effacées, ou corrompues à la suite d’un piratage. La mise en place de ce procédé vous assure qu’aucune donnée ne sera perdue quel que ce soit le cas de figure auquel nous ferions face. Nous voulons également vous préciser que ce processus ne ralentira en rien le système d’information, car ces sauvegardes se feraient en parallèle et ne « bloqueront » pas les données. Nous ferions également des sauvegardes sur des emplacements de stockage qui ne seront pas connecté à internet pour éviter toute intrusion, et assurer complétement la sécurisation des données. Ce périphérique de stockage sera placé dans une cage de Faraday. Qui est très utile lors d’une tempête électromagnétique. Une tempête électromagnétique est susceptible de détruire toutes les données présentes sur les éléments de stockages, qui seront situés sur son rayon d’action. Il est donc primordial de mettre en place un système similaire qui peut être fait soi-même, pour un coût extrêmement faible. Une ligne de contact en cas d’urgence disponible 24h/24h vous sera donnée. Une personne qui sera à votre écoute, et qui sera disponible pour effectuer des opérations d’urgence, ou de remise en place des données par exemple. Cette offre peut s’avérer très intéressante, notamment lorsque vos serveurs internes à l’entreprise sont devenus défectueux du jour au lendemain. Ceci est une des façons que l’on utilise pour assurer la continuité du service. Toute connexion passant sur nos serveurs est garantie, quel que soit l’outil que vous utilisez, vous pourrez toujours avoir quelqu’un à votre disposition et qui est prêt à vous aider en complément de ce cet engagement de qualité.

La sécurisation des données se fera également grâce à un mot de passe suffisamment long et complexe. Cela me permet de rebondir sur une autre de vos problématiques : « L’intrusion d’un client sur un poste d’une commerciale dépourvu de mot de passe ».

## 5.D La mise en place des bonnes pratiques

La problématique des mots de passe est quelque chose de très récurrent dans les entreprises, et cela reste un moyen extrêmement facile d’intrusions dans un réseau, un compte, une boîte mail, la comptabilité, la liste des identifiants... Un pirate novice peut en quelques clics trouver presque tous les mots de passe d’une société dans la majorité des cas. Il essayera d’abord, très certainement de trouver les mots de passe qui peuvent mette en péril la société. Imaginons qu’un pirate arrive à trouver le prix d’achat de vos véhicules, il pourra alors très simplement revendre ces données à vos concurrents, et ainsi s’aligneront sur vos prix, ou feront des prix plus compétitifs que les vôtres. Ces informations sont très convoitées car selon les cas, un fichier peut coûter plusieurs milliers, voire plusieurs millions d’euros. Nous avons de nombreux moyens d’éviter ce genre de cas de figure, nous pouvons par exemple obliger les utilisateurs à sélectionner un mot de passe sécurisant (en forçant les majuscules, les minuscules, les caractères spéciaux, les chiffres et un nombre de caractère minimum). Il est également fortement conseillé, d’obliger l’utilisateur a changé le mot de passe tous les 2 ou 3 mois par exemple. Le simple fait d’augmenter le nombre de caractères du mot de passe, peut faire varier le temps de « forçage » du mot de passe, de quelques secondes, à plusieurs milliers, voire plusieurs millions d’années. Ce temps de « forçage » est en réalité le temps que mettra le pirate pour trouver le mot de passe sans le connaître. Nous pourrions également mettre en place en parallèle, un système qui bloquera le compte, lorsqu’un trop grand nombre de tentative de renseignement de mot de passe sera effectué. Bien évidemment ce blocage de compte n’est pas définitif.



[Cette photo](http://www.zenzla.com/astuces/231-supprimer-le-mot-de-passe-de-session-window.html) par Auteur inconnu est soumis à la licence [CC BY-SA](https://creativecommons.org/licenses/by-sa/3.0/)

Nous pouvons également donner un mot de passe à l’utilisateur qui sera prédéfini, et qui lui sera impossible de changer, celui-ci pourrait être modifié automatiquement tous les 2 mois par exemple. Bien sûr, dans le règlement intérieur de l’entreprise, c’est écrit, qu’il est interdit de recopier ce mot de passe où que ce soit. Que ce soit sur un ordinateur ou sur un post-it, toute négligence pourra être sanctionnée, ne pas respecter ceci, rend toute « contrainte » concernant le mot de passe, presque inutile.

Si l’utilisation de plusieurs mots de passe est nécessaire, nous pouvons mettre en place une application qui sert de coffre-fort à mots de passe, qui est totalement sécurisé et non utilisée à des fins commerciales. Les mots de passe sont souvent les talons d’Achille des sociétés utilisant les outils informatiques.

Dans l’idéal, un mot de passe doit être défini pour chaque application ou chaque site. Cela permet de mettre différents « niveaux » de sécurité. Même si un mot de passe fuite, les autres applications ne seront pas touchées.

## 5.E Les comportements à travailler

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

Ce problème peut être résolu sans aucune intervention informatique, seulement un peu de prévention. Nos mainteneurs sont triés avec précautions afin qu’ils ne regardent pas, quelque chose qui ne leurs est pas destiné, ne modifient pas ou ne téléchargent pas vos documents confidentiels. Le fait de verrouiller les ordinateurs lors d’une opération qui ne nécessite pas d’intervention sur l’ordinateur peut être un moyen d’être certain qu’aucune donnée ne fuitera (lorsque le mot de passe n’est pas apparent), nous pouvons également mettre en place un système d’auto-déconnexion de session au bout de 15 minutes par exemple. Même si d’une façon ou d’une autre, un de nos informaticiens consulte un document confidentiel, notre charte informatique régit des règles, et il sera emmené en justice aura une lourde amende, très plausiblement une peine de prison et sera licencié de notre société.

Il n’y a aucun risque qu’un acte pareil reste impunis, car toutes les opérations de maintenances sont tracées, donc nous savons quel opérateur a été désigné ce jour-ci, et l’heure à laquelle il est arrivé dans vos locaux.

Une simple clé USB, CD ou disque dur par exemple, peut avoir des conséquences tragiques, les employés doivent à tout prix surveiller leurs ordinateurs, que ce soit un technicien ou un collègue. C’est pour cela que nous pourrions envisager une désactivation des ports USB pour toute l’entreprise. Bien sûr toute modification n’est pas permanente, et nous pouvons donc enlever l’interdiction sur certaines prises pour un certain temps ou pour toujours si le besoin est prouvé et validé par exemple.

## 5.F Conclusion

Bien que certaines de ces pratiques, peuvent impliquer des contraintes aux employés, nous avons vu que leurs mises en place est essentiel pour un bon fonctionnement du service informatique dans le temps. La moindre faute, ou la moindre inadvertance d’un collaborateur peut entraîner de très grave conséquence, pouvant aller jusqu’à la fermeture de l’entreprise. De simples gestes, une sensibilisation des utilisateurs, suivie par nos actions, sont des procédés plus que suffisantes au maintien du fonctionnement des différents systèmes de sauvegardes et de traitement de l’information.

***Synthèse sur l’utilisation de l’outil informatique en entreprise***

D’un point de vue général, une charte informatique doit contenir les règles d’utilisation par les salariés du système d’information et de communication de l’entreprise ainsi que les sanctions consécutives au non-respect de ces règles.

Par ailleurs, en tant que besoin, une charte informatique doit également permettre d’informer les salariés sur les procédés de surveillance mis en place par l’employeur et permettant notamment de dissuader les salariés d’utiliser les outils informatiques à des fins répréhensibles et non professionnel.

Il en ira de même de l’information des salariés relative aux risques d’infractions, qui peuvent être commises au moyen des outils informatiques de l'entreprise.

Enfin, l’employeur peut éventuellement, au sein de la charte informatique, s’exonérer, dans une certaine mesure, de la responsabilité qui lui incombe au titre de certaines infractions commises par ses salariés.

* Clause
* Sécurité
* Surveillance
* Infraction
* Aspect légal
* Interdits
* Validation

La validation s’effectue entre la DRH, La direction juridique, et les représentants des employés.

* Diffusion

Une fois rédigée et validée (selon le contenu retenu et l’organisation propre à chaque organisme : par la DRH, la Direction juridique, avec ou sans consultation des représentants du personnel), la charte doit être communiquée largement au sein de l’organisme via plusieurs modes de diffusion notamment :

* Document papier mis à disposition dans les locaux de l’entreprise
* En version numérique sur le réseau de l’entreprise
* Sur le site intranet de l’entreprise

# Charte Qualité Service Client

Condition Générales

Les règles définies ci-dessous ont pour objectif de réglementer et de définir les rapports entre la société de maintenance informatique, et le concessionnaire AutoConcept sur la prestation de services informatiques. La présente charte vise, via l’engagement de ses signataires, à fournir aux clients une qualité de service optimale sur le long terme et à établir des standards de qualité indispensable visant à maintenir un haut niveau de satisfaction de la clientèle.

Nos engagements

* Confidentialité

A défaut d’autorisation de la part du client, le respect de la confidentialité et de la non-exploitation des projets, des échanges, des données clients et numériques est garanti.

* Prestation de services

Nous nous engageons à être clair et explicite dans la description de la prestation fournie, pour laquelle nous possédons les compétences requises.

Tout au long de la prestation nous nous engageons :

* Informer le client sur les contraintes qui peuvent être provoqué pendant la prestation et donc freiner les travaux.
* Respecter les délais convenus au début des travaux dans la limite du possible.
* Conseil

Nous pouvons au besoin renseigner le client sur la législation en vigueur relative aux sites internet, logiciels ou supports numériques (licences, droits d’exploitation des logiciels…).

* Solution qualité

Nos techniciens mobiliseront toutes les forces et compétences nécessaires pour livrer des solutions de qualité qui répondront aux besoins et aux ressources du client, dans les délais impartis (tout retard ou manquement aux engagements convenus devant être justifié). Nous nous tenons informé des nouveautés web et multimédias, afin de proposer à nos clients des solutions actualisées et évolutives.

* Livraison

Nous nous engageons à livrer le produit ou service dans les délais impartis convenus préalablement avec le client, et à vous tenir au courant de chaque intervention. Nos techniciens testent et valident le bon fonctionnement des prestations réalisées, et doivent nous remettre sous la forme de leurs choix, les informations techniques relatives à tout matériel ou application livrée. Et doivent également vous donner une copie de ce rapport afin d’accompagner l’utilisateurs lors des différentes opérations.

* Assistance et support technique

L’accueil téléphonique est disponible du lundi au vendredi pour toute demande du client de 8h à 18h.En dehors de ces horaires un technicien d’astreinte sera à votre disposition 24/24h 7/7j.

Quel que soit le cas, une assistance pour la prise en main et un support technique de qualité seront fournis au client.

* Bonne conduite envers un client

Il est impératif d’avoir une bonne conduite envers un client c’est-à-dire de rester courtois, aimable, à l’écoute. Il est également impératif de respecter les horaires de rendez-vous les délais d’interventions. D’informer le client sur l’état de son pc et sur les opérations effectuées.



# Proposition de mémo interne

1. Une image contenant capture d’écran

   Description générée automatiquement

# Conclusion

Problématiques rencontrés par la société AutoConcept et solutions apportées.

Les différents points abordés dans le projet permettent de répondre aux problèmes remontés par le service commercial :

* La note de synthèse fait le point sur la bonne marche à suivre dans le cadre de l’utilisation de l’outil informatique et répond aux problèmes de sécurité lié aux mots de passe, d’intrusion sur les postes, de production en limitant les accès à certains sites et applications et la bonne conduite à tenir sur les logiciels utilisés en entreprise notamment les licences.
* La charte qualité promet un suivi et une qualité des interventions répondant aux problèmes d’attente ou de non-information des actions entreprises par les techniciens.
* Le plan de sécurisation, permet la sauvegarde des données, la protection des données et le changement rapide d’un poste évitant la perte de donnée/ productivité, généralement couteuse pour la société.
* Le mémo interne impose la conduite à tenir chez les clients répondant ainsi aux problématiques de tenues et d’attitude des techniciens chez le client.

# Annexe

***CHARTE INFORMATIQUE***

***INTERNE***

***Lire attentivement ce document pour lequel vous devrez signer une lettre de décharge le jour de votre intégration dans le groupe***

##### BONNES PRATIQUES D’UTILISATION DE L’E-MAIL ET D’INTERNET

Ce recueil a pour but d’établir les normes pour assurer l’usage acceptable de l’e-mail et des ressources d’Internet et de l’intégrité des systèmes d’information de la Société.

Les systèmes d’information, les ordinateurs et les données stockées font partie des actifs vitaux de l’entreprise. Ces actifs et leur bonne utilisation sont d’une importance primordiale pour la recherche d’informations, le transfert de connaissances, et l’amélioration des communications.

La Société accepte et encourage l’utilisation de l’e-mail et des services d’Internet pour supporter et conduire ses affaires. Toutefois, la Société doit se protéger des abus potentiels de ces systèmes et des risques afférents. Ce document décrit les pratiques à respecter dans l’utilisation du courrier électronique et Internet.

## Responsabilités

Tout employé de la Société et sa hiérarchie sont responsables de la protection de la Société et de ses actifs, contre les pertes et les dégradations, y compris, celles qui seraient dues à l’e-mail ou à l’Internet. A ce titre, vous devez respecter les normes et pratiques qui suivent. Le non-respect de celles-ci pourrait être considéré comme abusif.

## Bon usage

***… professionnel***

La Société met à votre disposition l’e-mail et/ou l’accès à Internet pour des besoins professionnels et vous encourage à utiliser ces outils pour votre travail et l’aider à gagner un avantage compétitif.

Utilisation de l’e-mail et de l’Internet :

* Contrôler les sites clés pour le développement de nos affaires
* Informer vos collègues des sites qui peuvent les aider dans leur travail
* Entretenir des relations d’affaire

Ne pas les utiliser pour :

* Envoyer du courrier en chaîne, participer à des jeux en ligne, télécharger des jeux, des économiseurs d’écran, de la musique, des logiciels et (sauf nécessité professionnelle) vous inscrire à des listes de diffusion, ou des groupes de discussion, ou envoyer des messages à des groupes d’échange
* Envoyer des informations sensibles commercialement sans cryptage adéquat, car Internet n’est pas un moyen de transport sûr.
* Répondre à des réclamations ou des demandes de renseignements arrivant par e-mail, à moins que ce ne soit de votre responsabilité de le faire.

***… personnel***

L’usage limité et occasionnel personnel est acceptable à la discrétion de votre hiérarchie. Cet usage doit se conformer à ces normes et pratiques.

***… convenances professionnelles***

Les conventions de courrier d’affaires doivent être utilisées pour composer et envoyer les messages e-mail et Internet comme s’il s’agissait de lettres et ou de notes écrites car ceux-ci sont aussi le reflet de notre professionnalisme.

## Interdits

Tout élément obscène, pornographique ou d’autre nature qui peuvent être choquants pour une autre personne – à caractère sexuel, raciste, sexiste, politique ou religieux qui comporterait des commentaires déplacés sur des orientations sexuelles, des handicaps ou des particularités personnelles est inacceptable.

Envoyer, Accéder, Visualiser, demander ou télécharger ce genre de documents est une infraction sérieuse à la politique de la Société en matière d’Internet et d’E-mail et peut constituer un délit. **Un rappel à l’ordre, voire des sanctions disciplinaires, pourront en résulter telles qu’elles sont définies dans le règlement intérieur, en relation avec la faute commise et dans le respect des droits de la défense.**

La récupération de fichiers auprès de sources inadéquates n’est pas autorisée, car elle présente le risque d’introduire des virus ou des logiciels piratés ou sans licence (jeux, économiseurs d’écran, exécutables). Les fichiers Vidéo ou audio ne sont pas autorisés sauf autorisation explicite de la hiérarchie.

## Aspect légal – Lois sur la copie

Les Lois sur la propriété intellectuelle s’appliquent aux e-mails et à tout ce qui circule sur Internet. Les éléments déposés ne doivent pas être téléchargés et mis en circulation.

## Surveillance

La Société se réserve le droit de contrôler le bon usage des règles d’utilisation des outils informatiques appartenant à l’entreprise dans le respect de la liberté individuelle de ses collaborateurs.

Le système de contrôle mis en place est justifié et proportionné au but recherché.

La taille maximale recommandée des fichiers transmis par messagerie électronique est de ***X*** Mo et la taille de la boîte courrier ne doit pas dépasser ***XX*** Mo.

Il vous est possible de contrôler vous-même la taille de votre boîte mail. Il vous suffit d’appliquer la procédure prévue à cet effet ou de contacter le service informatique.

Si vous recevez du courrier non sollicité ou déplacé, contactez le service informatique pour vous en débarrasser.

## Infractions

L’utilisation inappropriée, excessive, ou non autorisée de l’e-mail ou des services Internet est en infraction avec la politique de la Société et à ses normes et pratiques. Comme pour toute utilisation injustifiée, détournée ou non autorisée d’un outil mis à la disposition par le Groupe, tout abus commis en connaissance de cause est de nature à justifier une sanction telle que définie par le règlement intérieur, dans le respect des droits de la défense de l’intéressé.

## Informations complémentaires

Contactez le service informatique pour des avis, des conseils quant à la bonne utilisation du courrier électronique et de l’Internet, dans le cadre de ces normes et bonnes pratiques.

##### Lettre de décharge

***Lire attentivement la charte informatique annexée au règlement intérieur***

Madame, Monsieur,

Nous vous rappelons qu’en tant que salarié de la Société, vous êtes tenu de respecter les règles en vigueur dans l’entreprise.

Nous vous invitons à vous conformer aux bonnes pratiques d’utilisation de la messagerie électronique et d’Internet exposées dans la charte informatique.

Par la présente, vous déclarez avoir pris connaissance de cette Charte informatique et vous vous engagez à respecter les règles qui y sont notifiées.

Société :

Nom du salarié :

Date :

Signature :

Nb : Veuillez retourner cette note signée et datée au service informatique.

**Rappel des lois**

Il est rappelé que toute personne sur le sol français doit respecter la législation française y compris dans le domaine de la sécurité informatique :

*La protection des libertés individuelles*

La création de tout fichier contenant des informations nominatives doit faire l’objet d’une demande préalable auprès de la Commission Nationale de l’Informatique et des Libertés (CNIL). La loi 78-17 du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés et sa loi modificatrice 2004-801 du 6 août 2004 peuvent être trouvées sur le site.

La Directive 2002/58/CE du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques) s'applique plus spécifiquement au traitement des données à caractère personnel dans le secteur des télécommunications.

*Le respect du droit de propriété*

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quel qu’usage que ce soit. Les copies de sauvegarde sont les seules exceptions.

La copie d’un logiciel constitue le délit de contrefaçon sanctionné pénalement (code de la propriété intellectuelle). L’auteur d’une contrefaçon engage directement sa responsabilité, il peut être poursuivi devant les tribunaux répressifs et civils, la personne morale qui l’emploie.

*Le respect de l’intégrité d’un système informatique*

L’utilisateur s’engage à ne pas effectuer d'opérations pouvant nuire au fonctionnement du réseau, à l’intégrité de l’outil informatique et aux relations internes et externes de l’établissement.

La simple accession à un système sans autorisation constitue un délit, même s’il n’en est résulté aucune altération des données ou fonctionnement dudit système. Si de telles altérations sont constatées les sanctions prévues sont doublées.

Il est à souligner que de tels actes (même de simples tentatives) sont susceptibles d’entraîner l’éviction de la fonction publique.

La répression des atteintes aux systèmes de traitement automatisé de données est prévue par la loi du 5 janvier 1988 (Loi dite "Godfrain", du nom de son initiateur), dont les dispositions ont été reprises, depuis le premier mars 1994, par les articles 323-1 à 323-7 du Nouveau Code Pénal.

*Le respect du secret de la correspondance*

Les utilisateurs doivent s’abstenir de toute tentative d’intercepter les communications privées, qu’il s’agisse de courrier électronique ou de dialogue direct

La loi numéro 91-646 du 10 juillet 1991 stipule dans son article 2 : "Le secret des correspondances émises par la voie des télécommunications est garanti par la loi", sont concernés : le téléphone, le télécopieur, les liaisons informatiques et télématiques.

De lourdes sanctions pénales frappent celui qui porte atteinte au secret de la correspondance (Articles 226-15 et 432-9 du nouveau code pénal).

**Texte de loi**

Article 323-1 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004) Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 30000 euros d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 45000 euros d'amende.

Article 323-2 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004) Le fait d'entraver ou de fausser le fonctionnement d'un système de traitement automatisé de données est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

Article 323-3 :

(Ordonnance n° 2000-916 du 19 septembre 2000 art. 3 Journal Officiel du 22 septembre 2000 en vigueur le 1er janvier 2002)

(Loi nº 2004-575 du 21 juin 2004 art. 45 I Journal Officiel du 22 juin 2004) Le fait d'introduire frauduleusement des données dans un système de traitement automatisé ou de supprimer ou de modifier frauduleusement les données qu'il contient est puni de cinq ans d'emprisonnement et de 75000 euros d'amende.

**Sources des graphiques (à retravailler) :**

COPYRIGHT © 2018 Groupe Atlas (Magazine) Mar, 12/05/2015 - 17:39 Auteur inconnu [en ligne] consulté le 15/10/2018

<https://www.atlas-mag.net/article/la-cybercriminalite>

COPYRIGHT © 2018 RECORDED FUTURE, INC. par Filip Reesalu le 24/03/2016 [en ligne] consulté le 20/10/2018

<https://www.recordedfuture.com/europe-ransomware-analysis/>

CREATIVE COMMONS (CC) IBM, Cyber Security Intelligence 2016 Auteur inconnu [en ligne] consulté le 14/10/2018

<https://fr.statista.com/infographie/5007/la-plupart-des-cyberattaques-contre-les-entreprises-sont-dorigine-interne/>

**Sources des citations (à retravailler) :**

COPYRIGHT © 2018 Groupe Atlas (Magazine) Mar, 12/05/2015 - 17:39 Auteur inconnu [en ligne] consulté le 15/10/2018

<https://www.atlas-mag.net/article/la-cybercriminalite>

PDF : [GUIDE DES BONNES PRATIQUES DE L’INFORMATIQUE](file:///D:\CESI\SAS\Doc%20projet%20SAS\guide_cgpme_bonnes_pratiques.pdf) (lien à revoir lors de déplacement des docs, pas utilisé sur ce doc, pour conclusion ?)

**Source des images :** Images uniquement en : « Creative Commons » tirées de Word, utilisant le moteur de recherche : « Bing », Auteur inconnu sauf pour les images citées consultées le 22/10/2018.