Vincent LLAGONNE

Quentin FERNANDEZ

Nicolas MAUPIN

Projet SAS

2016/2017

SOMMAIRE

1 PRÉSENTATION DE L'ENTREPRISE

1.1 HISTORIQUE

DSI Provence, fondé en 2013 par 3 jeunes collaborateurs, est une entreprise de maintenance informatique et d'hébergement avec à sa charge plus d'une cinquantaine d'employés. La mission principale de DSI Provence est de gérer le parc informatique des sociétés ainsi que la protection de leurs données.

1.2 ASPECT JURIDIQUE

DSI Provence est une SARL basée sur Aix-en-Provence. DSI Provence travaille pour de grandes firmes, telles que TESLA, GROUPAMA ou bien AÉRO Consultant tout situé à Aix la Duranne.

1.3 OBJECTIFS DE NOTRE CONTRAT

- Maîtriser parfaitement votre infrastructure informatique
- Documenter l'architecture système et réseau
- Rédiger les procédures techniques
- Présenter des préconisations techniques et budgétaires
- Sécuriser les données sensibles ainsi que l'infrastructure
- Des interventions sur site rapide et efficace

A. Des interventions sur site rapide et efficace

À nous déplacer directement sur votre site en cas de problème qui ne peut être résolu à distance.

B. Hotline et télémaintenance :

Notre support technique s'engage à traiter votre demande pour tous incidents dans un délai de 15 minutes. Vous êtes mis en contact directement par notre équipe de techniciens hot-line où vous êtes recontacté dans les 30 min.

C. Sauvegarde et de sécurité

Dès le démarrage de notre prestation, nos ingénieurs mettent en place une stratégie de sécurité et de sauvegarde afin de prévenir les risques potentiels. Ainsi, vos données sont protégées et peuvent être restaurées en cas de problème. Nous utilisons des antivirus managés directement depuis nos consoles de supervision et nous mettons en place une politique de sauvegarde efficace (disque dur externe, serveur de stockage, sauvegarde dans notre Datacenter).

D. Supervision

Nous assurons une prestation de haute qualité via une maintenance préventive de supervision instantanée qui nous remonte des informations en temps réel sur l'état de votre parc informatique. Ainsi, nous sommes dans la mesure de vous garantir le bon fonctionnement de votre infrastructure

Optimisation de votre infrastructure.

Nos techniciens vous conseillent et suivent votre infrastructure dans un objectif constant d'amélioration.

1.4 LOGO ET PARTENAIRE

2 SYNTHÈSE SUR L'UTILISATION DE L'OUTIL INFORMATIQUE EN ENTREPRISE

DSI Provence s'engage à respecter les textes de loi, concernant la sécurité des fichiers, la protection de données des utilisateurs, le filtrage de flux internet qui transite au sein de l'entreprise par les utilisateurs. En leur communicant un annuaire de leurs droits d'accès, de rectifications et d'opposition.

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

Chaque employé doit être notamment informé :

- Des finalités poursuivies;
- Des destinataires des données;
- De son droit d'opposition pour motif légitime;
- De ses droits d'accès et de rectification.

Cette information peut se faire au moyen d'une charte, annexé ou non au règlement intérieur, d'une note individuelle ou d'une note de service...

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

- Accorder des droits d'accès selon l'utilisateur ;
- Choisir des mots de passe complexe se renouvelant régulièrement ;
- Sauvegarder régulièrement les données et les placer hors entreprise.

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

L'employeur doit informer ses salariés, préalablement à la mise en place d'un annuaire, de leurs droits d'accès, de rectification et d'opposition. Cette information s'effectue par la remise d'un document écrit ou par voie électronique (voir modèle proposé en annexe).

La diffusion sur internet de donné à caractère personnel (ex. : nom, prénom, coordonnées professionnelles, etc.) rend ces informations accessibles à quiconque, sans que l'intéressé puisse réellement maîtriser leur utilisation. Par conséquent, le salarié doit pouvoir s'opposer simplement et à tout moment à une telle diffusion.

La CNIL recommande que la diffusion de la photographie soit subordonnée à l'accord préalable de l'employé en particulier lorsque cette photographie est destinée à être publiée ou mise en ligne sur internet.

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

- Interdire l'accès à des sites illégaux via une solution de filtrage de contenus Web (protéger le réseau)
- L'entreprise doit s'engager à conserver les données de connexions (LOG) pendant 1 an
- Mise en place d'une charte informatique portée à la connaissance des salariés et du comité d'entreprise

Il y a une obligation de déclaration à la CNIL, sauf si le filtre internet ne permet pas un filtrage individualisé des salariés sont non obligatoires

3 ANALYSE COMPTE RENDU SERVICE COMMERCIAL

3.1 PROBLÈMES – IMPACTS – SOLUTIONS

A. Lenteur de certains postes :

- La lenteur de certain poste peut avoir un gros impacte sur la productivité et cette lenteur peut être du a un problème de disque dur et donc engendrer une perte de données.
- Changer le PC concerné s'il est trop vieux, faire une Upgrade ou faire une remise à zéro.

B. Crash de disque sans sauvegarde :

- On peut voir que dans le compte-rendu du service commercial qu'un crash de disque dur a coûté plus de 80 000€ les disques durs ont une durée de vie limitée. L'entreprise n'est pas à l'abri de re subir ce genre de problème qui peut lui causer encore une perte d'argent.
- Pour régler le problème d'un crash de disque, il faut externaliser les données personnelles et professionnelles. L'utilisation d'un NAS redondé peut totalement régler le problème de perte de données de l'entreprise. Il faut aussi réaliser une sauvegarde journalière sur bande de toutes les données.

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

- N'importe qui peut introduire un virus, copier des données sensibles, modifier des documents et supprimer vos données personnelles et professionnelles et donc engendrer encore une perte d'argent.
- Imposer un mot de passe composé de 8 caractères minimum avec Chiffre lettre majuscule/minuscule et caractères spéciaux. Ce mot de passe doit être modifié tous les 45-90 jours. Le mot de passe doit être personnel, il ne doit pas être transmis à un utilisateur ou administrateur.

D. Messages intempestifs de « version de Windows pirates » et problèmes de licence :

- L'utilisation d'une version de Windows ou autres logiciels piratée est certes gratuite, mais illégale. Mis à part le côté illégal une version piratée peut entraîner des problèmes techniques, contenir des virus, des bugs qui peuvent engendrer des pertes de données et donc entraîner une diminution du chiffre d'affaires. Sur le plan financier, la CNIL peut passer et déposer une amande ce qui entraîne encore une perte du chiffre d'affaires. Il peut aussi ternir l'image de la société et donc rendre les clients méfiants ce qui entraîne une perte de client et donc de chiffre d'affaires.

- Créer un mot de passe pour accéder au BIOS ce qui empêchera l'utilisateur d'installer une autre version de Windows. Créer un groupe utilisateur dans l'Active Directory pour qu'il ne puisse pas installer de programmes sans l'accord d'un administrateur.

Nous avons constaté qu'il y a beaucoup de plainte contre l'équipe technique :

Les plaintes :

- Des délais d'intervention anormalement longue.
- Des tenues non adapté pour le client
- Un mauvais accueil téléphonique
- Les clients ne sont pas au courant de l'avancement des interventions
- Les problèmes sont parfois non résolus
- Certain membre de l'équipe technique regarde et divulgue des données confidentielles

Nous avons donc pensé à rédiger un mémo interne ainsi qu'une charte client que nous nous engageons à respecter et à faire évoluer pour s'adapter à vos nouveaux besoins et palier à tous les problèmes que vous avait et allait rencontrer. (Voir annexe pour la charte client et le mémo interne)

4 GESTION DE STOCK, REMPLACEMENT POSTES ET PRÊT DE PC

- Référencer dans une base de données chaque matériel (Marques, date d'achat, lieu, adresse Mac). Par exemple GLPI
- Faire l'inventaire après chaque remplacement de poste
- Effectuer un prêt de matériels pour que le client puisse continuer à travailler pendant le délai d'intervention sur son poste défectueux
- Remplacer si possible le matériel défectueux par le même équipement ou similaire pour que le client ne soit pas « dépayser »
- Une fois que le matériel prêté n'est plus utilisé, l'utilisateur doit de rendre le matériel pour nous permettre de continuer un suivi du matériel.
- Sécuriser les locaux où sont situés les stocks avec un accès par code, badge ou clef

5 SAUVEGARDE

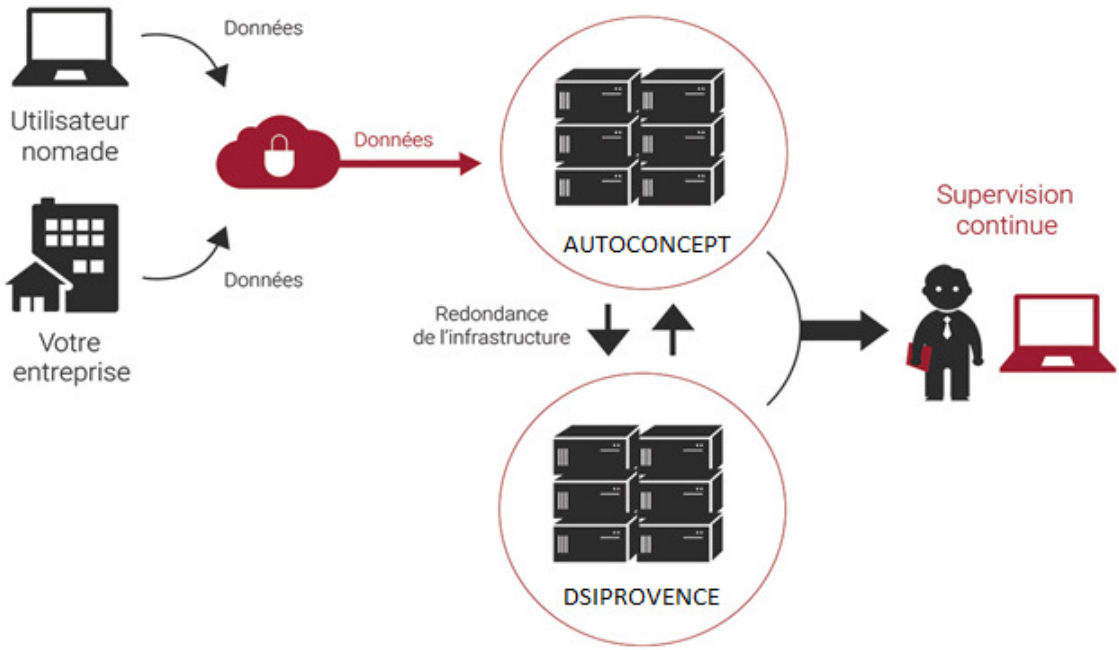
5.1 MODE DE SAUVEGARDE

Proposition 1 sauvegardée sur un serveur local + une copie dans notre entreprise (ce qu'on préconise)

- Un coût plus élevé
- Une copie de vos sauvegardes sont sécurisé dans notre data center
- Les deux bâtiments sont reliés par une fibre pour une synchronisation rapide des données

Proposition 2 externalisée sur un serveur Cloud les sauvegardes. (-coût, +sécurité, +temps)

- Le prix dépend de l'hébergeur
- Vos données sont enregistrées sur un Cloud sécurisé
- La vitesse de synchronisation dépend de votre débit internet



5.2 TYPE DE SAUVEGARDE

A. Sauvegarde complète

Toutes les données sont sauvegardées à chaque sauvegarde, qu'elle soit identique à la précédente ou non

Avantages : Ce type de sauvegarde permet la restauration la plus rapide

Inconvénient : Nécessite beaucoup d'espace de stockage

B. Sauvegarde incrémentielle

Ce mode de sauvegarde se base sur une sauvegarde complète préalablement effectuée. L'incrémentielle ne va sauvegarder que les fichiers qui ont été créés ou modifiés entre la sauvegarde complète et le début de la sauvegarde incrémentielle.

Avantages : Ce type de sauvegarde prend le moins d'espace de stockage

Inconvénient : Restauration longue

C. Solution proposée

Nous proposons une copie de vos données (dans une salle sécurisée) dans notre Datacenter, en plus d'être sauvegardés au sein de vos locaux.

Nous vous proposons une sauvegarde complète hebdomadaire et incrémentielle journalière pour vous assurer une sécurité optimale.

6 LE RAID

6.1 Qu'est-ce un RAID de disque?

Le système RAID permet de répartir des données entre plusieurs disques durs pour améliorer les performances, la sécurité ou la tolérance aux pannes du système

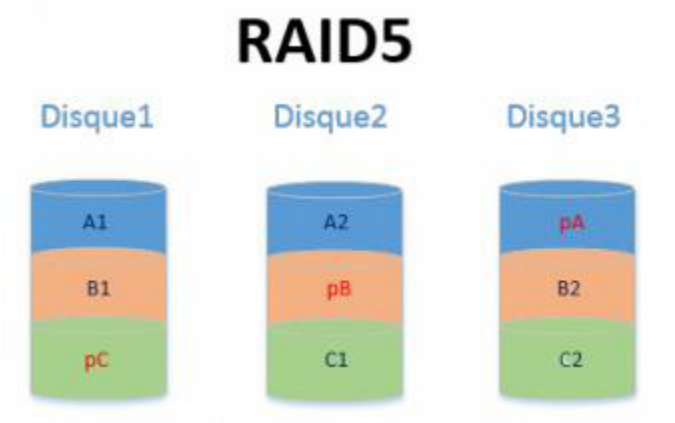
6.2 RAID proposé

RAID 5 :

Le RAID5 est une technologie visant à utiliser 'n' disques (au moins 3) de mêmes capacités, pour en faire un espace de stockage. La capacité est alors de n-1 disques, la capacité de l'un des disques est, en effet, sacrifiée afin de sécuriser la grappe (en anglais, on parle d'array). Ainsi, si vous disposez de 3 disques de 1To, votre RAID5 aura une capacité de 2To. Avec ce RAID, vous disposez d'une tolérance de panne d'un disque. Ce qui signifie que si un des disques lâche, vous ne perdrez pas vos données. En revanche, si 2 disques lâchent simultanément, toutes les données sont perdues.

- Les avantages :
  - Vous ne voyez qu'un seul volume
  - Les performances sont améliorées (performances en lecture équivalentes à un RAID 0)
  - Vous avez une tolérance de panne de 1 disque.

- Les inconvénients :
  - L'écriture est un peu moins performante du fait du calcul de parité
  - Vous perdez l'équivalent d'un disque, en termes d'espace de stockage (ex: 3 disques de 2 To donneront un espace de 4 To).
  - Nombre de disques minimum : 3



7 POLITIQUE DE CONFIDENTIALITÉ DE MOT DE PASSE

- Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts. En particulier, l'utilisation d'un même mot de passe pour sa messagerie professionnelle et pour sa messagerie personnelle est à proscrire impérativement.
- Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.).
- Ne demandez jamais à un tiers de créer pour vous un mot de passe.
- Modifiez systématiquement et au plus tôt les mots de passe par défaut lorsque les systèmes en contiennent.
- Renouvelez vos mots de passe avec une fréquence raisonnable. Tous les 90 jours est un bon compromis pour les systèmes contenant des données sensibles.
- Ne stockez pas les mots de passe dans un fichier sur un poste informatique particulièrement exposé au risque (exemple : en ligne sur internet), encore moins sur un papier facilement accessible.
- Ne vous n'envoyez pas vos propres mots de passe sur votre messagerie personnelle.
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis.

8 SOLUTION FILTRAGE

Utiliser un pare-feu permet de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique.

Le but est de fournir une connectivité contrôlée et maîtrisée entre des zones de différents niveaux de confiance, grâce à l'application de la politique de sécurité et d'un modèle de connexion basé sur le principe du moindre privilège, comme un accès interdit aux protocoles des messageries instantanées afin d'améliorer la productivité.

Exemple :

- YouTube
- Twitter
- Facebook
- jeux en ligne

9 Solution de reprise d'activité

9.1 PCA – PRA

A. Définition

PCA : Plan de continuité d'activité, organisation d'un Système Informatique pour assurer sa continuité en cas de panne majeure

PRA : En informatique, un plan de reprise d'activité permet d'assurer, en cas de crise majeure ou importante d'un centre informatique, la reconstruction de son infrastructure et la remise en route des applications supportant l'activité d'une organisation.

B. Risques potentiels

Les risques naturels et environnementaux :

- Séismes, inondations, éboulements, glissements de terrain
- Proximité de sites industriels, d'infrastructures ou de voies de communication à risque

Les risques techniques et humains :

- Pannes matérielles, indisponibilité d'équipements, défaillances logicielles, infections virales…
- Phénomènes sociétaux, mouvements sociaux, dégradations volontaires, erreurs humaines,

Indisponibilité de collaborateurs :

- Épidémie
- Mouvement social
- Accident

C. Solutions de prévention

- Redondance de la salle serveur sur le site de DSI Provence
- Une sauvegarde des données incrémentielle
- Une sauvegarde des données des utilisateurs sur le réseau
- Un stock conséquent pour pouvoir remplacer un PC défectueux sans avoir à en recommandé
- Gestion des prestataires
- Travaille à distance

DSI Provence

MÉMO

À : Service informatique

De : DSI Provence

Date : 7 novembre 2016

Re : Directive services informatique

---

1. Les techniciens se doivent d'intervenir en tenue correcte et soignée.
2. D'être toujours à l'écoute du client.
3. Gérer les priorités.
4. S'organiser un planning.
5. Lors d'une intervention, le technicien se doit d'être le plus clair possible pour expliquer la résolution des pannes sans rentrer dans des termes techniques.
6. Se doit de suivre les procédures lors d'une maintenance et installer uniquement des logiciels sous licence.
7. Respecter la vie privée du client.
8. Respecter et informer les délais d'intervention.
9. Référencer chaque produit dans une base de données pour un suivi du matériel (Model, numéro de série, licence, garantie …).
10. Centraliser les demandes des clients.
11. L'intervenant se doit de respecter les dossiers personnels des utilisateurs et de ne pas laisser de traces écrites ou informatique de mot de passe.
12. Ne pas prendre de pause pendant une intervention avec un client ou lors d'une maintenance critiques.

Charte Qualité client

Relationnel client

- Garantir la qualité des conditions de l'accueil en agence ou au téléphone.
- Une relation personnalisée, avec un interlocuteur identifié.
- Dès le premier accueil, vous délivrer une information claire sur notre identité, nos services, prestations et tarifications
- Un suivi adapté à vos besoins et attentes
- Vous écouter, vous conseiller et comprendre vos besoins pour vous apporter une solution correspondante à vos attentes
- Vous orienter vers le niveau de maintenance supérieur pour respecter nos délais
- Une enquête de satisfaction régulière

Sécurité et productivité

- Vous assurer un SLA adapté à vos besoins
- Sécuriser et garantir une confidentialité de vos données professionnelles.
- Vous assurer une prise en compte rapide de votre problème
- Un suivi efficace pour vous apporter une résolution du problème dans un délai raisonnable.
- Une salle serveur sécurisé et surveillé

Continuité de service

- Vous assurer un suivi de l'intervention : remplacement du technicien en cas d'indisponibilité
- Vous assurer une redondance de vos serveurs et données

Télécopie :
Téléphone :
Service technique :

Client : IP

* B I 0 0 0 0 0 1 9 7 5 7 5 *

No Intervention ou BCI :

Date :

RAPPORT D'INTERVENTION

Adresse d'intervention - Nom du contact - Téléphone

Tél :

Descriptif panne et travail demandé

Travail effectué / Compte rendu

Action à effectuer :

Observations client

Début prestation :

Fin prestation :

Temps passé :

Déplacement (temps) :

INTERVENANT(S)

Nom :

Signature :

CLIENT

Nom :

Signature :

Cachet :


CHARTE
INFORMATIQUE

Introduction

La présente charte a pour objet de définir les règles d'utilisation des moyens informatiques au sein des établissements du Groupe AUTOCONCEPT et de rappeler à chacun des utilisateurs ses responsabilités.

Ladite charte, associée au règlement intérieur du Groupe AUTOCONCEPT, est avant tout un code de bonne conduite. Elle a pour objet de préciser la responsabilité des utilisateurs en accord avec la législation afin d'instaurer un usage correct des ressources informatiques et des services internet, avec des règles minimales de respect d'autrui.

1. Définitions

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

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

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

2. Domaine d'application

Les règles et obligations énoncées dans la présente charte s'appliquent à tout utilisateur des ressources informatiques du Groupe AUTOCONCEPT (stagiaires, personnels administratifs ou techniques, entreprises externes, apprentis, intervenants externes, clients, etc.).

À ce titre, la présente charte doit être communiquée à tout utilisateur interne ou extérieur au Groupe AUTOCONCEPT utilisant ces ressources informatiques. La charte est diffusée à l'ensemble des utilisateurs et mise à disposition sur le panneau d'affichage des établissements.

Les contrats souscrits entre le Groupe AUTOCONCEPT et tout tiers donnant accès aux données, aux programmes informatiques ou à tout autre moyen du Groupe AUTOCONCEPT devront stipuler que ces utilisateurs s'engagent à respecter la présente charte. Les représentants des utilisateurs externes s'engagent à faire respecter la présente charte aux éventuelles entreprises sous-traitantes.

Ces ressources informatiques comprennent les serveurs, les stations de travail, les équipements mobiles, tout type de périphérique et les équipements pédagogiques situés dans les services administratifs, les locaux d'enseignement, les laboratoires, les hébergements externes et tout autre local du Groupe AUTOCONCEPT disposant de tels matériels.

Les installations du Groupe AUTOCONCEPT permettant de se connecter ou de dialoguer avec des sites informatiques dans le monde entier, les règles définies par la présente charte s'étendent également à l'utilisation des ressources des réseaux extérieurs, accessibles par l'intermédiaire de réseaux d'interconnexion comme internet.

Le non-respect des règles de bonne conduite énoncées dans la présente charte engage la responsabilité personnelle de l'utilisateur.

3. Respect de la déontologie informatique

3.1. Principes fondamentaux

Tout utilisateur est responsable de l'usage qu'il fait des ressources informatiques. Il doit particulièrement veiller à user raisonnablement de toutes les ressources partagées auxquelles il accède (puissance de calcul, espace disque, bande passante du réseau, internet, etc.).

L'utilisation des ressources informatiques partagées du Groupe AUTOCONCEPT et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, modem, borne d'accès sans fil, téléphone, etc.) sur le réseau sont soumises à autorisation du service informatique et aux règles de sécurité du Groupe AUTOCONCEPT. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité qui l'a justifiée. Toute connexion à une ressource informatique partagée avec les ressources informatiques pédagogiques du Groupe AUTOCONCEPT est proscrite.

Tout utilisateur s'engage à respecter les règles de déontologie informatique lors de l'utilisation de tout type de ressources informatiques et de tout type de médias de communication (web, réseaux sociaux, « microblogging », forum, tchat, etc.) et notamment à ne pas effectuer des opérations ayant pour but :

- De masquer sa véritable identité ;
- D'usurper l'identité d'autrui ;
- De s'approprier le mot de passe d'un autre utilisateur ;
- De mettre en place un programme pour contourner les procédures établies dans le but d'augmenter ou de diminuer le niveau de sécurité des ressources informatiques ;

- D’utiliser ou de développer des programmes mettant sciemment en cause l'intégrité des ressources informatiques ;
- D'installer et d'utiliser un logiciel à des fins non conformes aux missions du Groupe AUTOCONCEPT ;
- De ne pas respecter les règles d'accès aux salles contenant le matériel informatique ;
- D'utiliser des comptes autres que ceux auxquels il a légitimement accès ;
- D'utiliser un poste de travail ou tout autre ressource informatique sans une autorisation préalable du responsable de formation sous contrôle du service informatique ;
- D'accéder aux données d'autrui sans l'accord exprès des détenteurs, même lorsque ces données ne sont pas explicitement protégées.

L’évolution permanente des technologies de l’informatique met à disposition des utilisateurs de nouveaux services qui peuvent être accessibles depuis le réseau du Groupe AUTOCONCEPT. Ces nouvelles technologies, qui peuvent présenter un risque de vulnérabilité particulier, ne peuvent être utilisées qu’après accord préalable du service informatique et dans le strict respect de la présente charte.

3.2. Support de communication

L'usage des supports de communication électronique (courriers, forums de discussion, documents accessibles par le web, réseaux sociaux, « microblogging », tchat, etc.) doit se faire dans le respect des règles suivantes :

- Ne pas porter atteinte à l'intégrité, à l’image et à l’intérêt d'un autre utilisateur et/ou du Groupe AUTOCONCEPT, notamment par l'intermédiaire de messages, textes ou images provocants, diffamatoires ;
- Ne pas charger ou transmettre, sciemment, des fichiers contenant des virus ou des données altérées ;
- Préciser si l’expression est faite à titre personnel ou au nom du Groupe AUTOCONCEPT, d’une de ses composantes, et ce, particulièrement dans toute communication à diffusion publique.

L’utilisateur s’engage à ce qu’aucun contenu ne contienne de publication véhiculant des messages grossiers, insultants, diffamants à l’encontre d’autrui ou de propos ou images susceptibles de porter atteinte à l’ordre public, au respect de la personne humaine ou de sa dignité, à l’égalité entre les hommes et les femmes, à l’origine ethnique, à la protection des enfants et des adolescents ; des propos ou des images encourageants à commettre des crimes ou délits ou véhiculant des messages à caractère pornographique, ou faisant l’apologie ou la négation ou la remise en question des crimes de guerre et/ou contre l’humanité.

Par ailleurs, chacun devra s'assurer que les documents qu'il publie sont libres de droits et que les personnes figurant sur les photos et vidéos publiées ont donné leur accord explicite.

3.3. La protection des libertés individuelles

La création de tout fichier, bases de données, sites internet, services de réseaux sociaux, contenant des informations nominatives et/ou à caractère privé doit faire l'objet d'une demande et déclaration préalable auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

3.4. Le respect du droit de propriété

La législation interdit à tout utilisateur de faire des copies de logiciels commerciaux pour quelque usage que ce soit.

La copie d'un logiciel constitue le délit de contrefaçon.

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

En outre, dans les documents qu'il met à la disposition des tiers, l'utilisateur s'engage à respecter les droits d'auteur et ceux liés à la propriété intellectuelle.

L'utilisateur ne doit pas lire, modifier, copier ou détruire d'autres fichiers que ceux qui lui appartiennent en propre, directement ou indirectement.

3.5. Le respect de l'intégrité des ressources informatiques

Seuls les utilisateurs ayant eu l'autorisation préalable du service informatique pourront procéder à l'installation et à la mise à jour de logiciels, de pilotes ainsi qu'à l'ouverture des micro-ordinateurs du Groupe AUTOCONCEPT afin d'y ajouter un périphérique supplémentaire.

Les périphériques de médias amovibles (clé USB, disque dur externe, etc.) sont tolérés sous réserve qu'ils ne contiennent aucun logiciel malveillant.

La maintenance des postes est de la seule responsabilité du Groupe AUTOCONCEPT (pour les postes dont le Groupe AUTOCONCEPT est propriétaire). L'utilisateur n'a, en aucune façon, le droit de modifier la configuration matérielle des ressources informatiques sans que cela ne soit autorisé par le service informatique.

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

La simple accession aux ressources informatiques, sans autorisation, est répréhensible, même s'il n'en est résulté aucune altération des données ou fonctionnement des ressources informatiques. En cas d'altérations des sanctions sont prévues.

Les actes consistant à empêcher le fonctionnement d'une ou des ressources informatiques du Groupe AUTOCONCEPT, par exemple par l'introduction de virus ou par l'introduction ou la modification frauduleuse de données, sont répréhensibles.

La connexion et/ou l'utilisation à des services proxys en dehors de celui fourni par le réseau du Groupe AUTOCONCEPT, ainsi que l'usage de services de « tunneling » (Connexion réseaux privés virtuels ou l'encapsulation de données d'un protocole réseau dans un autre) sont interdits. Néanmoins, l'usage de ces deux types de service est possible sous les conditions suivantes :

- Uniquement après autorisation préalable du responsable pédagogique et du service informatique ;
- L'accès au service doit être exceptionnel et limité dans le temps.

Il est à souligner que la réalisation (même la simple tentative) des actes susvisés est susceptible d'entraîner l'éviction de l'école.

3.6. Le respect du secret de la correspondance

Les utilisateurs doivent s'abstenir de toute tentative d'interception de communications privées, sous quelques formes qu'elles soient.

Toute violation du secret de la correspondance, sous quelques formes qu'elle soit, est répréhensible.

3.7. Le dépôt légal

La loi prévoit que « les progiciels, les bases de données, les systèmes experts et les autres produits de l'intelligence artificielle sont soumis à l'obligation du dépôt légal dès lors qu'ils sont mis à la disposition du public ».

Par conséquent, les produits réalisés au sein d'un service et mis à la disposition du public sont soumis à l'obligation du dépôt légal. Cette formalité doit être respectée sous peine de sanctions.

3.8. L'usage de la cryptographie

La cryptographie peut se définir comme suit : « On entend par prestation de cryptographie, toutes prestations visant à transformer à l'aide de conventions secrètes des informations ou signaux clairs en informations ou signaux inintelligibles pour des tiers, ou à réaliser l'opération inverse, grâce à des moyens matériels ou logiciels conçus à cet effet. On entend par moyen de cryptographie, tout matériel ou logiciel conçu ou modifié dans le même objectif ».

Toute personne qui procède au codage, à la cryptographie, de tout moyen de communication qu'elle entend transmettre par la voie des télécommunications doit respecter les procédures prévues par la loi, d'autorisation ou d'agrément préalable, sous peine de sanctions.

3.9. Contenu des informations

Les informations diffusées sur tout type de médias de communication et sur tout type de réseaux (informatique, web, réseaux sociaux, « microblogging », forum, tchat, etc.) ne doivent pas :

- Porter atteinte à la vie privée ou à l'image d'autrui, sous quelques formes que ce soit ;
- Ne pas effectuer de diffamations ou d'injures, à l'encontre de qui que ce soit et sous quelques formes que ce soit;
- Contrevenir aux lois sur la propriété intellectuelle, littéraire et artistique ;
- Faire l'apologie de tout type de crime ou délit (racisme, antisémitisme, etc.).

3. Accès aux ressources informatiques

Le droit d'accès est limité à des activités conformes aux missions du Groupe AUTOCONCEPT, notamment :

- La certification des personnes ;
- La recherche scientifique et technologique ainsi que la valorisation de ses résultats;
- La diffusion de la culture et de l'information scientifique et technique ;
- La coopération internationale ;
- Les activités professionnelles.

Par ailleurs, l'étendue des ressources informatiques auxquelles l'utilisateur a accès peut être limitée en fonction des besoins réels et des contraintes imposées par le partage et/ou accès de ces ressources avec les autres utilisateurs.

Le droit d'accès est temporaire, il est retiré si la qualité de l'utilisateur ne le justifie plus.

Il peut également être retiré, par mesure conservatoire du responsable d'établissement, si le comportement d'un utilisateur n'est plus compatible avec les règles énoncées dans la présente charte.

Dans certains cas, un compte personnel peut être attribué. Ce compte est strictement personnel. Chaque utilisateur est responsable de l'utilisation qui en est faite. Nul n'est autorisé à utiliser le compte d'autrui.

Le mot de passe constitue la clé personnelle d'utilisation du compte et par conséquent ne doit être communiqué à personne (y compris à un administrateur).

5. Droits et devoirs

5.1. Des utilisateurs

La sécurité est l'affaire de tous, chaque utilisateur des ressources informatiques et du réseau du Groupe AUTOCONCEPT doit y contribuer en suivant ces règles :

- Ne pas masquer sa véritable identité ;
- Ne pas usurper l'identité d'autrui ;
- Choisir un mot de passe sûr et gardé secret ;
- Ne jamais donner son mot de passe à un tiers (y compris à un administrateur système) ;
- Ne pas afficher de mot de passe, même si le poste de travail est partagé par plusieurs personnes ;
- Changer régulièrement de mot de passe ;
- Ne pas quitter son poste de travail en laissant une session en cours ;
- Ne jamais prêter son compte ;
- Ne pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités ;
- Ne pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède ;
- Ne pas utiliser les ressources informatiques du Groupe AUTOCONCEPT et/ou des ressources informatiques privées pour proposer ou rendre accessible aux tiers des données et informations confidentielles ou contraires à la législation en vigueur ;
- Ne pas déposer des documents sur un serveur sauf si celui-ci le permet ou sans y être autorisé par les responsables habilités ;
- Assurer la protection de ses informations (l'utilisateur est responsable des droits qu'il donne aux autres utilisateurs)
- Protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition ;
- Signaler aux administrateurs système toute violation, tentative de violation ou toute violation suspectée des ressources informatiques et de façon générale, toute anomalie constatée (mauvaise gestion des protections, faille système, logiciel suspect, etc.) pouvant nuire au bon niveau de sécurité des ressources informatiques ;
- Ne pas charger, stocker, falsifier, diffuser ou distribuer ou consulter sciemment au moyen des ressources de l'entreprise, des documents, informations, images, vidéos :

    → Contraires aux bonnes mœurs ou susceptible de porter atteinte au respect de la personne humaine et de sa dignité ;

→ Portant atteinte aux ressources du Groupe AUTOCONCEPT et plus particulièrement à l'intégrité et à la conservation des données du Groupe AUTOCONCEPT.

- Ne pas utiliser les ressources informatiques du Groupe AUTOCONCEPT à des fins de harcèlement, menace ou injure, et, de manière générale, violer les droits en vigueur ;
- Ne pas détourner des informations propres au Groupe AUTOCONCEPT à des fins de concurrence déloyale, d'émettre de fausses déclarations visant à falsifier les données du Groupe AUTOCONCEPT, de supprimer ou de modifier des données au préjudice du Groupe AUTOCONCEPT ;
- Protéger ses ressources informatiques privées d'un antivirus récent et avec la dernière mise à jour.

5.1. Des administrateurs des systèmes informatiques

Les administrateurs des ressources informatiques du Groupe AUTOCONCEPT ont le devoir d'assurer un bon fonctionnement des réseaux et des ressources informatiques. Ils ont le droit de prendre toutes dispositions nécessaires pour assumer cette responsabilité tout en respectant la déontologie professionnelle.

En particulier, les administrateurs des systèmes peuvent être amenés à examiner le contenu de fichiers ou boîtes aux lettres, et ce afin d'obtenir suffisamment d'informations pour pallier les incidents de fonctionnement ou dans le but de pouvoir déterminer si un utilisateur ne respecte pas la politique d'utilisation des ressources informatiques du Groupe AUTOCONCEPT décrite dans la présente charte.

Les administrateurs des systèmes ont l'obligation de préserver la confidentialité des informations privées qu'ils sont amenés à connaître dans ce cadre.

Les utilisateurs peuvent demander l'aide des administrateurs systèmes pour faire respecter leurs droits.

5.3. Utilisation des logiciels

L'utilisateur ne peut installer un logiciel qu'après accord du service informatique compétent.

L'utilisateur ne devra en aucun cas :

- Sans l'accord précité, installer des logiciels ;
- Faire une copie d'un logiciel commercial ;
- Contourner les restrictions d'utilisation d'un logiciel ;
- Développer des programmes constituant ou s'apparentant à des virus.

5.4. Utilisation des ressources informatiques

Chaque utilisateur s'engage à prendre soin du matériel et des locaux informatiques mis à sa disposition. Il informe le service informatique de toute anomalie constatée.

L'utilisateur doit s'efforcer de n'occuper que la quantité d'espace disque qui lui est strictement nécessaire et d'utiliser de façon optimale les moyens de compression des fichiers dont il dispose.

L'utilisation des ressources informatiques doit être rationnelle et loyale afin d'en éviter la saturation.

Toute ressource informatique propre à un département, laboratoire, service, ou tout local du Groupe AUTOCONCEPT, doit être connectée au réseau par l'intermédiaire d'un technicien informatique du Groupe AUTOCONCEPT. Ce dernier s'assure en particulier que les règles de sécurité sont bien respectées.

Un utilisateur ne doit jamais quitter un poste de travail en libre-service sans se déconnecter.

5.5. Gestion des boîtes aux lettres électroniques

L'AUTOCONCEPT met à disposition une messagerie électronique fonctionnant avec Microsoft Office 365. Cette messagerie fonctionnant avec le domaine internet viaDSIProvence.fr est à destination du personnel.

Tout utilisateur s'engage à utiliser le service pour un usage professionnelle et personnel et ne doit pas envoyer des messages en masse, en chaîne ou à des fins commerciale (exemple : messages reçus individuellement dans le cadre d'une diffusion collective avec invitation à les renvoyer

également collectivement).

Les administrateurs de la messagerie pourront être amenés à faire évoluer le service ou à modifier certains paramétrages des boites aux lettres. Pour éviter des dysfonctionnements du service de messagerie, et pour des raisons de maintenance, le service peut être coupé temporairement.

D'une façon plus générale, des modifications des paramètres de messagerie pourront être faites pour assurer le fonctionnement.

Le service protection et de prévention des données des utilisateurs sont pilotés suivants les conditions techniques de Microsoft Office 365.

En cas d'inactivité de l'utilisateur, le AUTOCONCEPT se réserve le droit de supprimer le compte et les services périphériques et leurs contenus.

5.6. Accès à internet

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

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

L'accès internet est sécurisé et surveillé par :

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

Quotidiennement un contrôle de consommation de données utilisateurs à internet est effectué. Ce contrôle porte sur les sites visités, les durées des connexions et la bande passante consommée.

Le filtrage et la surveillance de ces connexions est permanent. Ceux-ci ne peuvent être débloqués qu'à des fins pédagogiques après accord du service informatique et du responsable pédagogique.

En cas de surconsommation d'internet ou de souci de sécurité, le service informatique peut alerter le responsable de formation ou tuteur et le Directeur régional afin de faire appliquer la présente charte.

Le Groupe AUTOCONCEPT se réserve tout droit de fermer l'accès à des sites ou à des services internet pour assurer la protection et la disponibilité du réseau internet à ses utilisateurs.

Le Groupe AUTOCONCEPT se réserve le droit de fermer la connexion internet sans préavis avec l'accord du Directeur régional pour assurer la protection de son réseau professionnel.

5.8. Fichiers de journaux de traces, analyse et contrôle de l'utilisation des ressources informatiques

Pour des nécessités de maintenance et de gestion technique, l'utilisation des ressources matérielles ou logicielles ainsi que les échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment de la loi sur l'informatique et les libertés.

La totalité des services utilisés génèrent, à l'occasion de leur emploi, "des fichiers de traces".

Ces fichiers sont essentiels à l'administration des systèmes.

En effet, ils servent à remédier aux dysfonctionnements des services ou systèmes informatiques utilisés. Ces fichiers conservent des informations concernant, par exemple, la messagerie (expéditeur, destinataire(s), date), mais aussi heures de connexion aux applications, au service de connexion à distance, numéro de la machine depuis laquelle les services sont utilisés, etc.

Ces types de trace existent pour tout le périmètre d'usage des services internet. Ces fichiers ne sont utilisés que pour un usage technique et d'indicateurs d'usages.

Les personnels en charge des opérations de contrôle sont soumis à une obligation de confidentialité. Ils ne peuvent donc divulguer les informations qu'ils sont amenés à connaître dans le cadre de leur fonction, en particulier lorsqu'elles sont couvertes par les secrets des correspondances ou relèvent de la vie privée de l'utilisateur, dès lors que ces informations ne remettent en cause ni le bon fonctionnement technique des applications, ni leur sécurité, ni l'intérêt du Groupe AUTOCONCEPT.

5.9. Les pare-feu / firewall

Les pare-feu vérifient tout le trafic sortant du Groupe AUTOCONCEPT, aussi bien local que distant. Ils vérifient également le trafic entrant constitué de la messagerie électronique, et/ou l'échange de fichiers, et/ou la navigation sur internet.

Ils détiennent toutes les traces de l'activité qui transite par eux :

- S'agissant de la navigation sur internet (sites visités, heures des visites, éléments téléchargés et leur nature texte, image, vidéo ou logiciels) ;
- S'agissant des messages envoyés et reçus (expéditeur, destinataires, objet, nature de la pièce jointe, et éventuellement texte du message).

Ils filtrent 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, ou contenant des données jugées comme offensantes, piratage, hacking et cracking.

5.10. Durée de conservation des données

La durée de rétention des messages électroniques supprimés et courriers indésirables, liés à l'utilisation de la boite aux lettres électronique fournie par le Groupe AUTOCONCEPT, est au maximum de 14 jours.

Les données présentes sur les serveurs professionnels sont stockées et conservées durant la période de formation puis supprimées suivant les conditions de la charte d'usage d'Office 365.

Il est à la charge de l'utilisateur de sauvegarder ses données avant la fin de sa formation.

Les fichiers de journaux de traces (c'est-à-dire un enregistrement dans des fichiers « logs », confère paragraphe *5.8* de la présente charte) des activités des utilisateurs, des anomalies et des événements liés à la sécurité. Ces journaux d'événements sont conservés sur une période glissante ne pouvant excéder 6 mois (sauf obligation légale ou demande de la CNIL de conserver ces informations pour une durée plus longue).

6. Sanctions

Les utilisateurs ne respectant pas les règles et obligations définies dans la présente charte et ceux qui ne signalent pas les tentatives de violation de leur compte sont passibles de sanctions :

- Ils peuvent être sommairement déconnectés par les administrateurs systèmes qui peuvent surveiller en détail des sessions de travail d'un utilisateur s'il existe un soupçon de non-respect de la présente charte
- Leur compte peut être fermé, sur décision du responsable ;
- Ils peuvent être convoqués devant le conseil de discipline ;
- Ils peuvent faire l'objet de poursuites judiciaires.

6. Adhésion de la charte et aux chartes d'usages des services

L'acceptation de la présente charte du bon usage des ressources informatiques et du réseau du groupe AutoConcept induit l'acceptation sans réserves des conditions générales d'utilisation des services numériques et des chartes d'usage qui leurs sont associés.

L'utilisation d'un service numérique entraine l'acceptation de sa propre charte ou conditions générale sans réserves de la part de l'utilisateur.

8. Durée de validité et révision de la charte

Le Groupe AutoConcept se réserve le droit, à sa seule discrétion et sans information préalable, de modifier, supprimer ou ajouter des clauses a ses chartes, et ce à tout moment. Il est donc conseillé aux utilisateurs de se référer régulièrement après acceptation à la dernière version des dits documents. La présente charte du bon usage des ressources informatiques et du réseau du groupe AutoConcept rentre en vigueur dès son acceptation par l'utilisateur et jusqu'à sa prochaine révision.

Je soussigné (nom et prénom) ……...,

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

Fait le ……..., à ……..,

En deux exemplaires originaux,

Signature (*lu et approuvé* à indiquer en mention manuscrite)