



# Security System

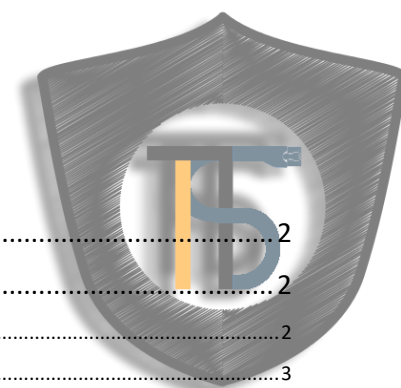
InformaTics Safety

## Dossier AutoConcept

GMSI PROJET SAS



# I. TABLE DES MATIERES



<b>II. ITS ET AUTOCONCEPT.....</b>	<b>2</b>
<b>INFORMATICS SAFETY .....</b>	<b>2</b>
INFORMATIONS LEGALES.....	2
NOTRE ACTIVITE .....	3
<b>AUTOCONCEPT .....</b>	<b>5</b>
INFORMATIONS LEGALES.....	5
VOTRE ACTIVITE ET VOS OBJECTIFS .....	7
<b>III. LE CAS AUTOCONCEPT .....</b>	<b>8</b>
<b>PROBLEMATIQUES INTERNES .....</b>	<b>8</b>
FINANCIERES.....	8
TECHNIQUES.....	8
HUMAINES.....	8
RESUME.....	9
<b>NOS PRECONISATIONS .....</b>	<b>10</b>
LOGICIELLES.....	10
GESTION ET STRATEGIE .....	10
SUIVI ET MAINTENANCE .....	11
RESUME.....	12
<b>IV. UTILISATION ET SECURISATION .....</b>	<b>13</b>
<b>REGLES D'UTILISATION DU MATERIEL INFORMATIQUE EN ENTREPRISE .....</b>	<b>13</b>
SOLUTIONS DE FILTRAGE DU CONTENU EN ENTREPRISE.....	13
<b>PLAN DE PREVENTION A LA SECURITE INFORMATIQUE .....</b>	<b>14</b>
<b>PLAN DE SECURISATION DES DONNEES.....</b>	<b>15</b>
SECURISATION PAR MOTS DE PASSE .....	15
PROTECTION ET SAUVEGARDE DES DONNEES.....	16
<b>V. NOS GARANTIES .....</b>	<b>18</b>
<b>NOTRE CHARTE QUALITE.....</b>	<b>18</b>
<b>MEMO INTERNE DE NOS AGENTS.....</b>	<b>19</b>
<b>VI. ANNEXES.....</b>	<b>20</b>
<b>ANNEXE 1 : INVENTAIRE MATERIEL ET LOGICIEL AUTOCONCEPT.....</b>	<b>20</b>
<b>ANNEXE 2 : CHARTE INFORMATIQUE TYPE .....</b>	<b>21</b>
<b>ANNEXE 3 : LEGISLATION ASSOCIEE.....</b>	<b>29</b>
<b>ANNEXE 4 : DISPOSITIF DE PREVENTION A LA SECURITE INFORMATIQUE.....</b>	<b>31</b>
<b>ANNEXE 5 : GLOSSAIRE.....</b>	<b>32</b>
.....	33

## II. ITS ET AUTOCONCEPT

INFORMATICS SAFETY

INFORMATIONS LEGALES



<b>Dénomination :</b> InformaTics Safety	<b>SIRET :</b> 810 859 322 000 10
<b>Adresse :</b> 2 Avenue Jean Moulin, 90000 Belfort, ZT Techn'Hom	<b>Activité (Code NAF ou APE) :</b> 5812Z
<b>Dirigeant :</b> M LAMBERT Laurent	<b>Forme juridique :</b> SARL
	<b>Immatriculation RCS :</b> 01/09/1982
<b>Chiffre d'affaires en 2017 :</b> 535 000 €	

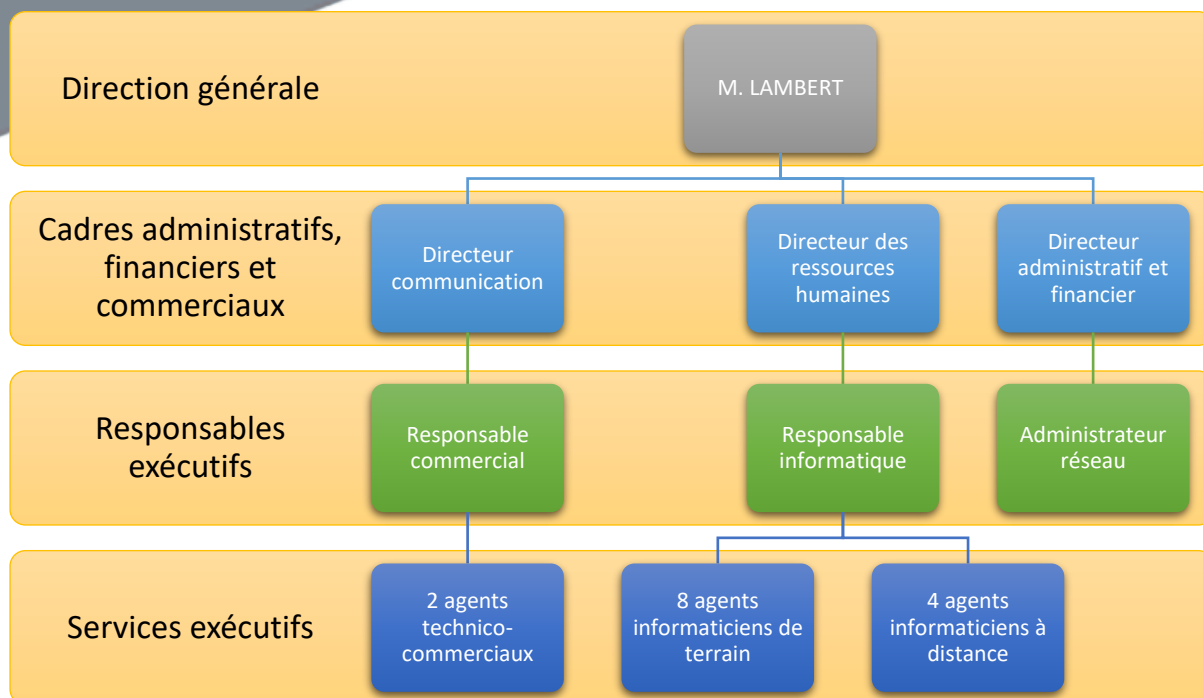


Depuis sa fondation en 1982 par Monsieur LAMBERT Laurent, la société ITS intervient depuis lors en tant que spécialiste des systèmes réseau, de leur sécurité ainsi que du matériel associé.

Elle rassemble aujourd'hui 21 collaborateurs répartis comme suit au sein de l'établissement :

- 7 membres encadrants ;
- 14 spécialistes au service direct de vos réseaux et parcs informatiques.

Dans le but de vous satisfaire au mieux, ces derniers se retrouvent déployés dans nos 3 services de la manière suivante :



## NOTRE ACTIVITE

Le rôle des différents membres de la société est de procéder ou vous conseiller dans la mise en place matérielle ou logicielle de votre réseau, l'administration ou la configuration de vos serveurs (Stockage, mail...), le dépannage ou l'entretien de votre parc informatique ainsi que dans la mise en place d'outils de sécurité et de sécurisation, notamment des données, afin de vous garantir la sérénité au quotidien.

L'entreprise, connaissant une croissance régulière de ses activités intervient auprès de ses clients dans le cadre de contrats ponctuels mais aussi dans le cadre de contrats annuels. Ces derniers nous ont permis d'entretenir une relation de confiance stable avec nos différents partenaires.

Grâce à notre implantation en plein cœur de la zone technologique de Belfort, nous avons pu établir de nombreuses collaborations dans les régions d'Alsace-Lorraine, de Bourgogne-Franche-Comté ainsi que du sud de la Champagne-Ardenne. Ce choix d'implantation nous permet d'intervenir sur site auprès de nos différents collaborateurs en 2 heures maximum dans le cadre d'une intervention technique nécessitant le déplacement d'un de nos agents.



Bien entendu, nous sommes aussi capables d'intervenir immédiatement, grâce à notre service technique téléphonique et à notre logiciel de prise en main à distance développé par nos soins.

Afin que chacune de nos interventions soit transparente pour vous, nous disposons par ailleurs de multiples outils de gestion, de suivi et d'information que nous mettons à votre disposition sur notre site internet <https://itsafety.com> :

- Outil en ligne de suivi des incidents et des demandes d'intervention ;
- Service téléphonique d'aide à distance disponible 24h/24, 7j/7 au 03 84 90 21 01 ;
- Plateforme en ligne de prévention aux risques informatiques ;
- Logiciel propriétaire de connexion à distance ;
- Liste de nos partenaires agréés (Pour du matériel, des logiciels ou des services fiables).





**Dénomination :** AutoConcept

**SIRET :** 016 950 339 000 24

**Adresse :** 5 Boulevard de l'Europe,  
21800 QUETIGNY

**Activité (Code NAF ou APE) :**  
4511Z

**Dirigeant :** M BLANC Pascal

**Forme juridique :** SARL

**Immatriculation RCS :** 02/06/1992

**Chiffre d'affaires en 2017 :** 5 000 000 €

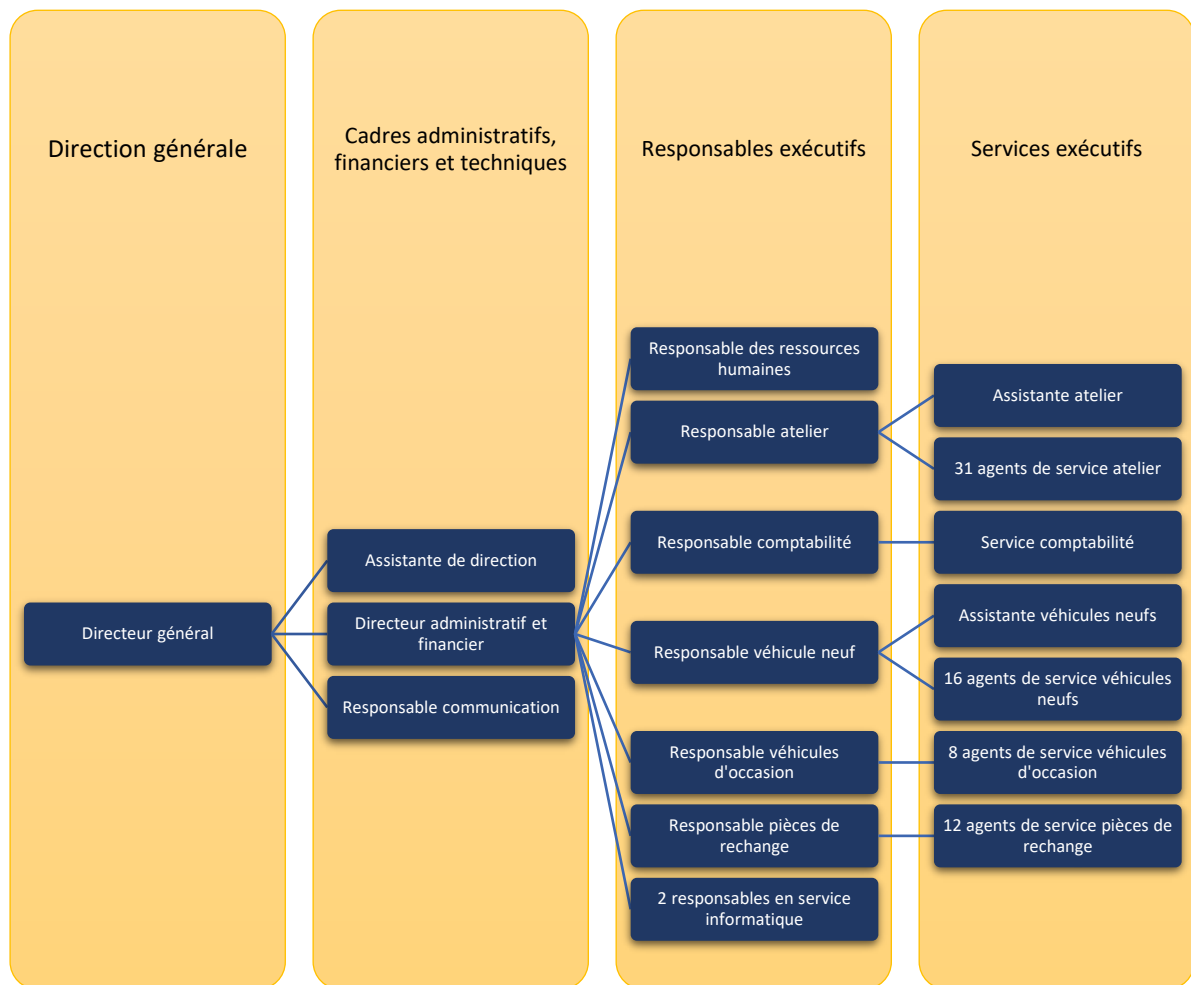


Depuis sa création en 1992 par Monsieur BLANC Pascal, la société AutoConcept évolue depuis lors en tant que garagiste concessionnaire sur les marchés du neuf et de l'occasion.



Elle rassemble aujourd'hui une équipe de 83 collaborateurs répartis comme suit au sein de l'établissement :

- 33 employés rattachés au secteur atelier ;
- 9 salariés au sein du service de comptabilité ;
- 17 professionnels dans le secteur des véhicules neufs ;
- 4 spécialistes sur la branche des véhicules d'occasion ;
- 13 personnes sous contrat assurant le fonctionnement du secteur des services ;
- 5 cadres supérieurs ;
- 2 techniciens en informatique.





La société détient un parc informatique relativement étendu, comprenant entre 70 à 80 postes informatiques.

Cependant, sur la totalité des postes inclus dans le parc de la société, seuls 68 postes sont occupés.

Parmi ces postes, il s'avère que les salariés de tous les services, hormis l'atelier, possèdent un poste informatique qui leur est propre.

Aujourd'hui, AutoConcept, confrontée à de nombreuses problématiques internes relatives à la bonne utilisation de son parc informatique ainsi qu'à son entretien, cherche à externaliser son service informatique ainsi que la gestion dudit parc, la concurrence dans son domaine d'activité ne leur permettant pas d'assurer ; à terme ; la bonne maintenance de ce dernier.

De nombreuses entreprises se sont déjà mises en concurrence sur l'appel d'offre lancé.



### III. LE CAS AUTOCONCEPT

#### PROBLEMATIQUES INTERNES



Aujourd'hui, nous distinguons trois catégories majeures parmi les problématiques rencontrées par AutoConcept dans la bonne gestion et maintenance de son parc informatique. La première relève du domaine financier, la seconde du domaine technique et enfin, du domaine humain.

Afin de mieux cerner ces différentes problématiques, en voici une liste non exhaustive ainsi que leurs implications vis-à-vis de notre champ d'intervention.

#### FINANCIERES

A ce niveau, nous allons tout d'abord être confrontés au récent renouvellement du parc informatique de la société. En effet, le service comptabilité de la société AutoConcept a imposé une période d'amortissement du matériel d'une durée de trois ans, ce qui implique qu'aucun changement matériel n'est envisageable. Afin d'optimiser nos interventions, un inventaire non exhaustif du matériel informatique faisant partie du parc sera à réaliser, ainsi que des logiciels nécessaires à l'activité de la société (Ref. Annexe 1).

De plus, toute immobilisation matérielle, soit-elle liée à une panne matérielle ou à une intervention technique, entraîne de graves perturbations dans le cadre de l'activité et la compétitivité de la société. Sur les événements ayant imposé une immobilisation matérielle, AutoConcept a constaté une perte de contrat se chiffrant à 60 000€ ainsi qu'une perte d'exploitation de 80 000€. Il est donc inconcevable d'imposer une intervention de longue durée privant le personnel d'un accès aux machines ou mettant en danger les données que celles-ci renferment.

Cependant, bien que tout changement ou immobilisation du matériel soient envisageables, rien n'exclut un investissement potentiel dans du matériel supplémentaire.

#### TECHNIQUES

D'un point de vue technique, la société possède un parc informatique suffisamment conséquent pour couvrir les besoins de transmission des informations entre ses différents services. Cependant, certains postes souffrent de ralentissement de leur système. Bien que peu impactant sur la sécurité des données, cette problématique de nature technique, porte atteinte à la bonne transmission de ces dernières ainsi qu'à la productivité des employés de la société.

Par ailleurs, la société AutoConcept est actuellement en situation légale précaire (Ref. Annexe 4) du fait de l'apparition de messages récurrents et intempestifs notifiant de l'absence de licence des systèmes sur certains postes. Ce point impacte à la fois la productivité mais aussi la crédibilité de la société.

En effet, la notion même d'absence de licence sur des postes professionnels est synonyme de vol pour tout client potentiel.

Par ailleurs, cela signifie aussi que la société AutoConcept ne peut exploiter la force du background afin de communiquer en temps réel avec ses différents membres sur des sujets concernant la société entière.

#### HUMAINES

Il apparaît assez clairement dans l'appel d'offre que certains salariés de la société AutoConcept soient coutumiers de l'utilisation de logiciels tiers (MSN entre-autres) allant à l'encontre de la productivité de la société, et ce, jusqu'à en avertir le service informatique lors d'un

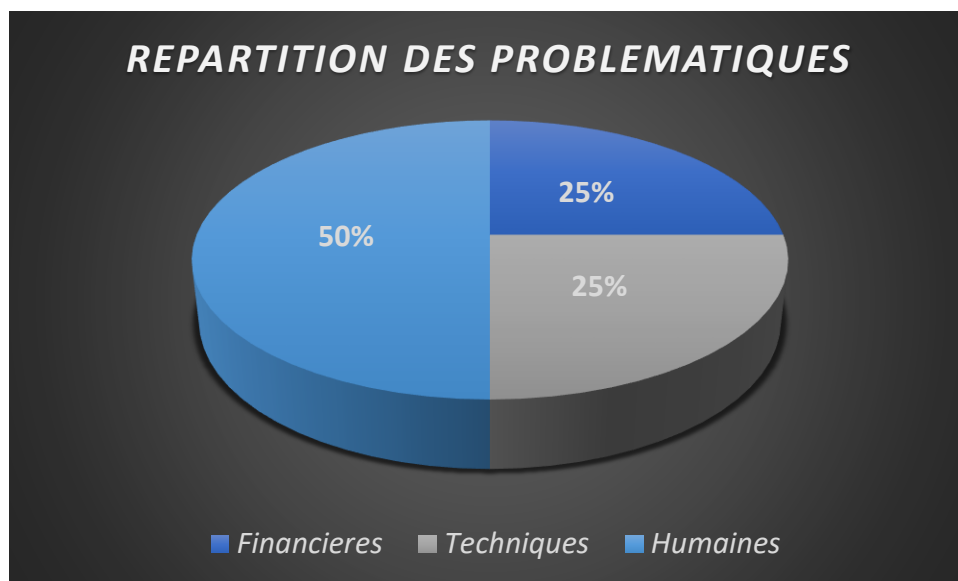
dysfonctionnement de ces derniers, au détriment du fait que la direction de l'établissement n'en cautionne pas l'usage. Une redéfinition claire des droits et obligations au sein de la société autour de la bonne pratique en informatique semble ici s'imposer.

De plus, la société AutoConcept est confrontée à de nombreuses fuites de données en son propre sein, notamment du fait de l'absence de mots de passe sur les postes informatiques. Il conviendra donc d'établir un dispositif de sécurité sur le parc informatique de la société et, bien entendu, faire participer chacun de ses membres à une campagne de prévention aux risques liés à la sécurité informatique.

Enfin, de nombreux utilisateurs se plaignent du service informatique, plus particulièrement de son sérieux et sa rapidité en intervention (Tenue inadaptée, délais inacceptables et indéterminés, demandes non prises en charge, mauvais accueil téléphonique, communication difficile étant donné la complexité technique du langage technique...). A ce niveau, nos équipes sauront parfaitement pallier à ce point en vertu de notre charte qualité et de la formation de nos agents (Ref. Nos garanties 1 et 2).

#### RESUME

Hormis la contrainte financière liée à l'achat récent du matériel informatique de la société ainsi qu'aux enjeux financiers de leur contenu, il s'avère que les problèmes rencontrés par la société AutoConcept relèvent majoritairement d'une gestion approximative de son parc informatique, ainsi que du laxisme de la direction envers ses employés quant à l'utilisation du matériel qu'il met à leur disposition.



Nous devons donc orienter notre intervention sur la restructuration de leur réseau interne en incluant un système de sécurisation de leurs données et de restrictions à leur accès tout en proposant, en parallèle, une formation de l'intégralité du personnel, direction incluse, aux bonnes pratiques de l'informatique en entreprise.

Comme vous pourrez le constater dans le chapitre suivant, notre intervention sera principalement structurelle et engendrera un coût moindre pour AutoConcept du fait du faible investissement matériel nécessaire pour répondre à l'intégralité de ses problématiques.

## NOS PRECONISATIONS

Afin de répondre aux différentes problématiques soulevées par le bilan établi par la société AutoConcept, nous préconisons la mise en place des différentes mesures qui suivent à différents niveaux.

### LOGICIELLES

Tout d'abord, il nous est primordial de définir quelles actions logicielles nous devons mener. Ainsi, en s'appuyant sur l'inventaire réalisé en Annexe 1 lors de notre première visite ainsi que sur le relevé des différentes problématiques rencontrées par AutoConcept, nous pouvons mettre en place les actions suivantes :

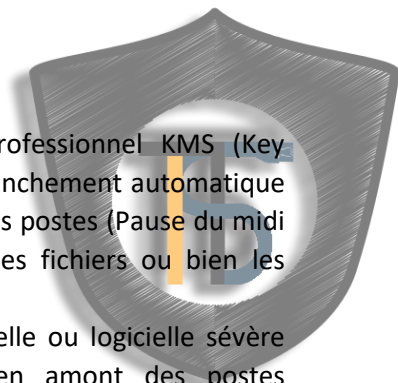
- Problèmes de licences : Application d'une licence officielle.
- Lenteur des postes : Mise en place d'un système logiciel de mise à jour et nettoyage automatisé des postes (Glary Utilities Pro).
- Personnel utilisant des applications contre-productives : Mise en place d'un système de filtrage d'applications et/ou des sites web.
- Problèmes de réactivité sur des interventions logicielles : Mise en place d'un système de prise en main à distance des postes de la société AutoConcept par le biais de notre logiciel propriétaire ITShare (Similaire à TeamViewer) afin de résoudre en temps un temps record les problèmes de moindre importance avec accompagnement téléphonique par un de nos techniciens.

### GESTION ET STRATEGIE

Grâce aux interventions logicielles, nous avons considérablement réduit le nombre de problématiques soulevées par la société AutoConcept. Cependant, les interventions logicielles ne sont pas suffisantes pour traiter l'intégrité des requêtes de cette dernière. La redéfinition d'une stratégie de gestion du parc informatique est nécessaire afin d'optimiser nos interventions logicielles et, au-delà de ça, déployer un système de sécurité efficace pour la société à travers la mise en place des actions suivantes :

- Lenteur des postes et pannes matérielles : Mise en place d'un système de stockage des données en ligne (Cloud) avec sauvegarde régulière afin d'alléger l'encombrement fichier des machines et prévenir des pertes de données en cas de panne matérielle.
- Problèmes de sécurité liés à des intrusions sur postes : Instauration d'un système de verrouillage des postes par mot de passe complexe, prédéfini et non modifiable, sous consultation individuelle de chaque salarié concerné par le dispositif.
- Problèmes de sécurité liés à des intrusions sur postes : Paramétrage de la mise en veille automatique des postes, et donc, leur verrouillage, au bout d'une durée d'inactivité déterminée en accord avec la direction de AutoConcept (Préconisation d'une durée maximale de 5 minutes).
- Impossibilité d'immobiliser les postes en cas d'intervention logicielle ou matérielle : Le parc de l'entreprise comptabilisant plus de postes que nécessaire, il faut donc employer un des postes libres en tant que « centre » du réseau de l'entreprise. A partir de ce dernier, les techniciens intervenants sur les postes de la société AutoConcept pourront donc intervenir depuis celui-ci sans à avoir à « débaucher » les salariés dont les postes rencontrent des problèmes. Cette mesure peut entre-autres permettre l'application





massive des licences officielles Microsoft via le système professionnel KMS (Key Management System) fourni par ces derniers ; favoriser le déclenchement automatique ou manuel d'actions logicielles hors des horaires d'activité sur les postes (Pause du midi par exemple) afin d'effectuer les mises à jour, les sauvegardes fichiers ou bien les nettoyages des postes.

- Impossibilité d'immobiliser les postes en cas de panne matérielle ou logicielle sévère entraînant l'incapacité à utiliser l'un d'eux : Préparation en amont des postes « inutilisés » de la société via le poste central afin de maintenir chacune de ces derniers à jour en cas d'immobilisation nécessaire et irrémédiable d'un des postes de service grâce à la technique du mastering dont le plan est établi grâce à l'inventaire logiciel qui sera réalisé (Ref. Annexe 1). Un remplacement immédiat et temporaire du poste immobilisé devient alors réalisable sans impacter sur la productivité de la société.

### *SUIVI ET MAINTENANCE*

Par ailleurs, il s'avère que la société AutoConcept rencontre de sérieux problèmes d'interaction avec son propre service informatique. De par notre charte qualité et notre mémo interne, nous sommes à même de garantir la résolution de ces problématiques.

De plus, dans le cadre du suivi et la maintenance du parc informatique de la société AutoConcept, notamment dans la résolution de ses problèmes de délais, nous proposons les services suivants :

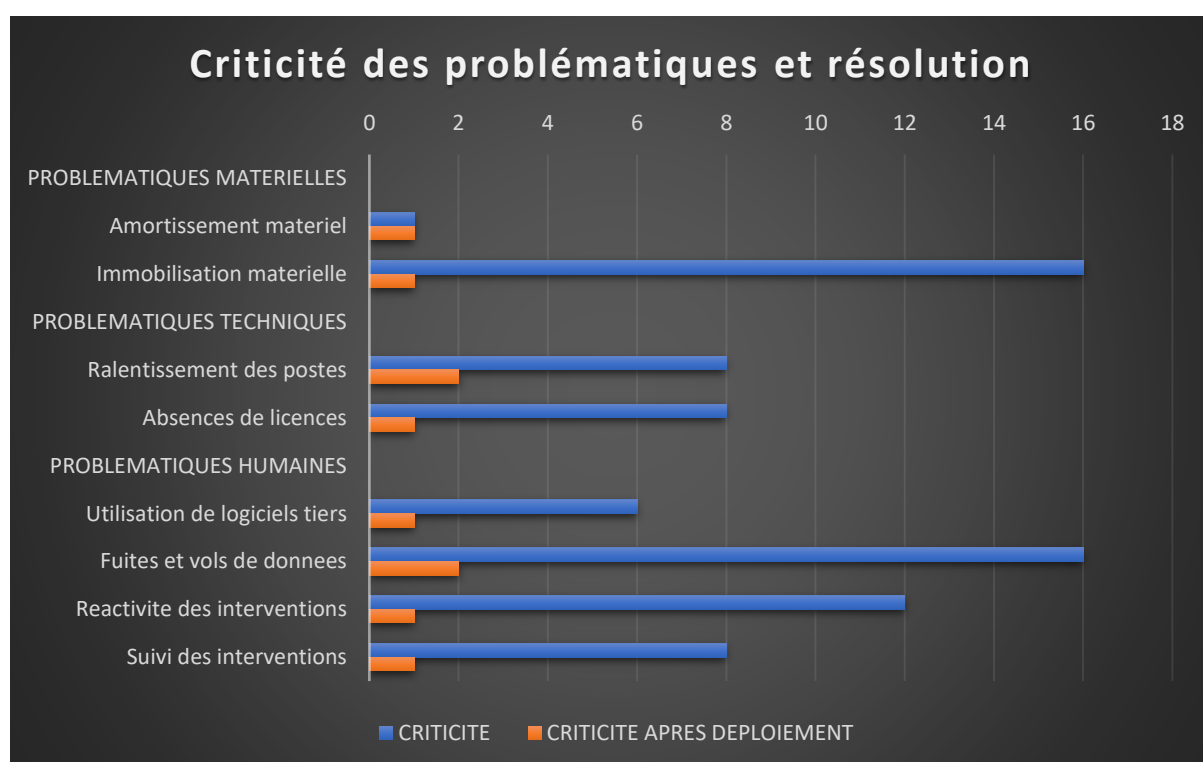
- Problèmes de communication relatifs aux problèmes techniques et matériels sur les postes : Délivrance ou envoi en formation du personnel de la section informatique vis-à-vis des relations humaines et de la bonne pratique de l'informatique en entreprise.
- Problèmes de communication vis-à-vis des interventions réalisées en cas de problème sur un poste ainsi que de réactivité et de tenue (vestimentaire et attitude) du personnel de la section informatique : Mise en place d'un système de gestion de tickets interne et externe (<https://itsafety.com/my-account/requests/>) visant à prioriser les interventions selon leur degré d'impact sur la productivité et la compétitivité de la société. Ce système, ouvert à tous les employés utilisant des postes, permettra alors un suivi en temps réel sur les interventions, dans un langage accessible à tous ainsi qu'une conservation de l'historique de ces dernières en vue d'établir de futurs points d'amélioration du parc informatique de la société.
- Problèmes de réactivité sur les interventions logicielles : 4 de nos techniciens sont disponibles 24/24, 7/7 par voie téléphonique au 03 84 90 21 01 afin de vous assister de manière pédagogique à la résolution de vos problèmes logiciels mineurs ainsi que sur le chat disponible sur notre site internet au lien suivant : <https://itsafety.com>

## RESUME

Ainsi, à la suite du déploiement de notre dispositif d'intervention, la société AutoConcept constaterait une amélioration colossale au sein de son parc informatique, qui lui permettrait alors de poursuivre son activité en toute sérénité.

Afin de souligner l'efficacité de nos méthodes, nous avons pris la liberté de mener une étude des risques basée sur les problématiques de la société indiquant une diminution colossale de 86% des risques de problèmes sur le parc informatique.

PROBLEMATIQUES	PROBABILITE	NIVEAU D'IMPACT	CRITICITE	CRITICITE APRES DEPLOIEMENT	REDUCTION
<b>PROBLEMATIQUES MATERIELLES</b>					
Amortissement materiel	1	1	1	1	0%
Immobilisation materielk	4	4	16	1	94%
<b>PROBLEMATIQUES TECHNIQUES</b>					
Ralentissement des poste:	4	2	8	2	75%
Absences de licence	2	4	8	1	88%
<b>PROBLEMATIQUES HUMAINES</b>					
Utilisation de logiciels tier:	3	2	6	1	83%
Fuites et vols de donnee	4	4	16	2	88%
Reactivite des intervention	3	4	12	1	92%
Suivi des interventions	4	2	8	1	88%





## IV. UTILISATION ET SECURISATION

### *REGLES D'UTILISATION DU MATERIEL INFORMATIQUE EN ENTREPRISE*

L'utilisation des outils informatiques sur le lieu de travail à des fins autres que professionnelles est généralement tolérée. Cette dernière doit être modérée et ne pas affecter :

- La sécurité et l'intégrité des réseaux de l'entreprise ;
- La productivité au sein de l'entreprise.

L'employeur est en droit de fixer, à sa convenance, des conditions et restrictions à l'utilisation de l'internet et des applications associées. Ces limites ne constituent en aucun cas une atteinte aux droits et à la vie privée des salariés.

Dans le cadre de l'édition de limites de tolérance vis-à-vis de l'utilisation des services informatiques en entreprise, l'employeur est en droit de consulter l'historique de navigation d'un salarié ainsi que ses mails (Hors mails personnels, se référer plus bas), en sa présence ou non. Dès l'instant où des limites ou restrictions sont appliquées, l'employeur est tenu d'annexer au règlement intérieur de l'entreprise ces dernières ou bien, les communiquer via une note de service générale.

Il lui est par ailleurs possible de désigner un délégué à la protection des données (DPO) qui sera associé à la mise en œuvre de dispositifs de contrôle.

En cas de difficultés ou de doute, il est recommandé de saisir l'inspection du travail, le procureur de la République ou le service des plaintes de la CNIL (Commission Nationale Informatique et Libertés) faisant office en tant qu'autorités compétentes reconnues en vertu des droits relatifs aux outils informatiques et à leur utilisation.

### *SOLUTIONS DE FILTRAGE DU CONTENU EN ENTREPRISE*

Les salariés doivent être informés de tout dispositif de contrôle de l'utilisation de l'outil informatique au sein de l'entreprise ainsi que de ses modalités. Les instances représentatives du personnel doivent préalablement être informées ou consultées avant déploiement de ces mesures.

Chaque salarié doit par ailleurs être informé et sensibilisé aux points suivants :

- Finalités poursuivies par la mise en place du dispositif (Productivité, sécurité, confidentialité...);
- Base légale d'application des modalités du dispositif relativement au Code du Travail, Code Civil et lois relatives à l'informatique, aux fichiers et aux libertés ;
- En cas de conservation des données, de la durée de conservation de ces dernières ainsi que de leurs destinataires ;
- L'existence du Droit d'opposition à l'enregistrement ou à la conservation de ces données ainsi qu'à leur accès et à leur rectification ;
- La possibilité de procéder à une réclamation auprès de la CNIL en cas d'irrespect d'un de leurs droits ou d'une mauvaise application de la réglementation relative à l'outil informatique.

L'employeur ne peut consulter les courriers ou les fichiers privés de ses salariés, même s'ils sont stockés sur le lieu de travail dès lors qu'ils sont formellement identifiés comme privés ou personnels et stockés dans un dossier formellement identifié de la même manière.

Cette protection est levée dans le cadre d'une enquête judiciaire en cours (Employé accusé de détournement de fonds, d'espionnage industriel...) ou bien, si l'employeur a su obtenir une décision de la part d'un juge l'autorisant à accéder à ces fichiers ou messages.

Les identifiants de chaque salarié sont strictement confidentiels. Cependant, en cas d'absence de ce dernier, si les informations contenues sur le poste de l'employé sont nécessaires à l'activité immédiate de l'entreprise, l'employeur est en droit de les exiger afin de maintenir le bon fonctionnement interne de sa société.

### *PLAN DE PREVENTION A LA SECURITE INFORMATIQUE*

Dans le but de s'assurer que tous les membres actifs d'une société soient avisés à propos d'un sujet précis, il est crucial de mettre en place des actions générales telles que des réunions ou des campagnes.

Ainsi, afin de sensibiliser l'ensemble des salariés d'AutoConcept au sujet de la sécurité des données, ITS s'engage à délivrer une période de sensibilisation sous forme d'une réunion générale regroupant tout le personnel, d'une durée de 2 heures adaptable.

Au cours de cette dernière, nous reprendrons avec chacun des salariés et dirigeants de la société les règles de bonne pratique de l'informatique en entreprise que nous rapporterons aussi au domaine privé.

De plus, durant cette réunion, des vidéos provenant du site internet du gouvernement relatif à la sécurité informatique <https://www.cybermalveillance.gouv.fr> seront diffusées afin d'illustrer nos propos.

Par ailleurs, à l'issue de la première partie de la réunion, nous appuierons sur nos propos avec les résultats de notre expérience humaine à la sécurité informatique que nous aurons mis en place dès notre arrivée dans les locaux de la société AutoConcept (Ref. Annexe 3).

Suite au débrief de cette expérience, un temps de parole visant à répondre à différentes interrogations sera alloué à tous les membres du personnel de la société.

Bien que de telles réunions soient suffisantes pour sensibiliser le personnel, des rappels à ces bien-fondés seront bien entendu remis à la direction de la société, sous forme d'affiches au format A3 qui pourront être affichées dans divers points stratégiques des locaux de l'établissement (Ref. Annexe 4).

Enfin, ITS met à disposition de ses partenaires une plateforme d'information et de formation en matière de sécurité informatique, délivrant de manière mensuelle une newsletter contenant des astuces indispensables pour optimiser votre sécurité interne ou personnelle ainsi qu'augmenter la vigilance de vos équipiers. Vous pouvez dès à présent en obtenir un aperçu en vous rendant sur notre page <https://itsafety.com/protect-yourself/>.

## PLAN DE SECURISATION DES DONNEES

Au sein d'une société, les dirigeants et salariés disposent de divers moyens de protection relatifs aux données de l'entreprise ainsi qu'à leurs données personnelles. Ces moyens dont ils disposent passent par différents processus que voici :

- L'adoption d'une politique rigoureuse de verrouillage des postes par mot de passe.
- La sécurisation des postes de travail et leur verrouillage en dehors des périodes d'activité.
- La détermination et l'identification précises des différents acteurs ayant accès aux fichiers.
- L'assurance de confidentialité des données accessibles aux prestataires.
- L'anticipation des risques liés à la perte ou à la divulgation des données.
- La sécurisation du réseau interne (réseau local) de la société ainsi que des locaux notamment à travers l'utilisation d'un VPN, le bon paramétrage du pare-feu et l'édition de ses règles ainsi qu'à l'installation d'un antivirus fiable sur les différentes machines amenées à être connectées au parc informatique de la société.
- La sensibilisation des utilisateurs aux risques informatiques ainsi qu'à leurs droits (Loi « informatique et libertés »).
- L'anticipation et la formalisation d'une politique de sécurité du système d'information à l'égard des points précédents.

### SECURISATION PAR MOTS DE PASSE

Afin de sécuriser les données informatiques, il est tout d'abord recommandé l'utilisation d'un mot de passe appliqué à la session des postes informatiques.

Dans le but d'offrir une protection maximale, il est fortement conseillé de remplir les critères suivants lors de sa création :

- Contenir un minimum de 8 caractères ;
- Intégrer au moins un caractère spécial (&, %, !, @, ...)
- Mélanger des caractères en minuscules et en majuscules
- Intégrer au moins un caractère numérique (1, 2, 3...)
- Que votre mot de passe ne figure pas dans un dictionnaire (Quelle que soit la langue).
- Que votre mot de passe ne soit pas en lien direct avec vous (Date de naissance, nom de l'animal de compagnie...)

Bien que la sécurité procurée par un tel mot de passe soit particulièrement efficace, son édition ne se limite pas uniquement à sa création seule.

En effet, un mot de passe se doit d'être unique et ne pas être employé pour différents postes ou services. Lors de sa création, vous pouvez utiliser des moyens mnémotechniques afin d'éviter un oubli futur comme suit ci-dessous :

« Mon boss est génial » : **M0nb0ss&g3n!4l**

En règle générale, le mot de passe par défaut défini lors de la création de votre identifiant en entreprise respecte les normes de sécurité recommandées. Il est alors conseillé de le conserver tel quel.

## PROTECTION ET SAUVEGARDE DES DONNEES

Au-delà de la protection des données par mot de passe, cette dernière passe par différents réflexes quotidiens à acquérir.

En effet, vos données, bien que protégées par mot de passe en dehors de vos heures d'activité, restent vulnérables en interne dès votre première connexion de la journée (Collègue jaloux ou malintentionné, prestataire trop curieux...).

De fait, afin de pallier à ce genre de situations, il est tout d'abord nécessaire que dès que vous quittez votre poste (Pour quelque motif ou durée que ce soient), vous verrouilliez votre session (« Touche Windows » + « L » ou bien via le menu Windows). Ainsi, vous seul avez accès aux données consultables depuis votre poste.

*Errare humanum est*, aussi est-ce pour cela qu'en cas d'oubli éventuel de verrouillage de votre session, il est vivement conseillé de mettre en place le système de verrouillage automatique de session après un temps prédéterminé d'inactivité (5 minutes maximum).

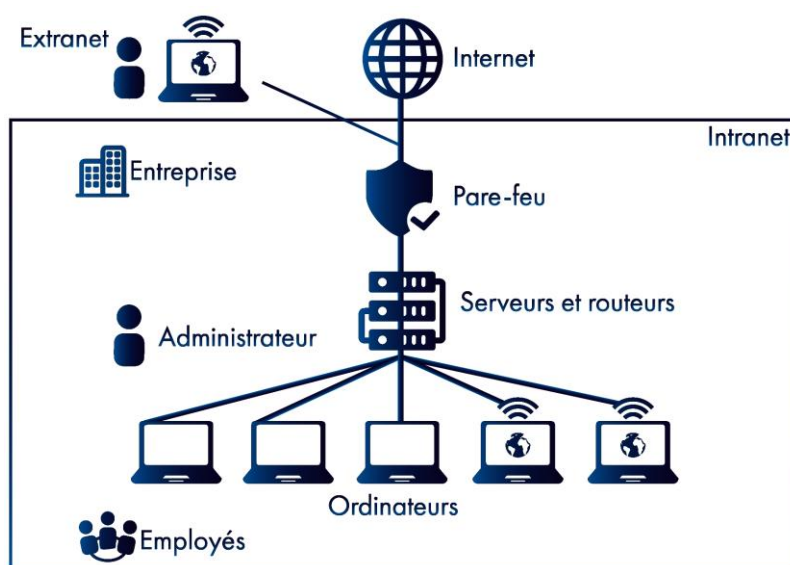
Par ailleurs, la sécurisation des données de votre entreprise peut aussi être renforcée par un système de centralisation et de stockage sur un dispositif interne chiffré ou en ligne (Serveur chiffré ou Cloud).

Afin de mettre cela en place, votre employeur ou administrateur réseau doit mettre en place une routine de sauvegarde régulière (Horaire ou quotidienne selon le trafic de fichiers sur votre poste) à partir d'un dossier partagé en serveur, qui, par souci d'accessibilité, sera placé sur votre bureau.

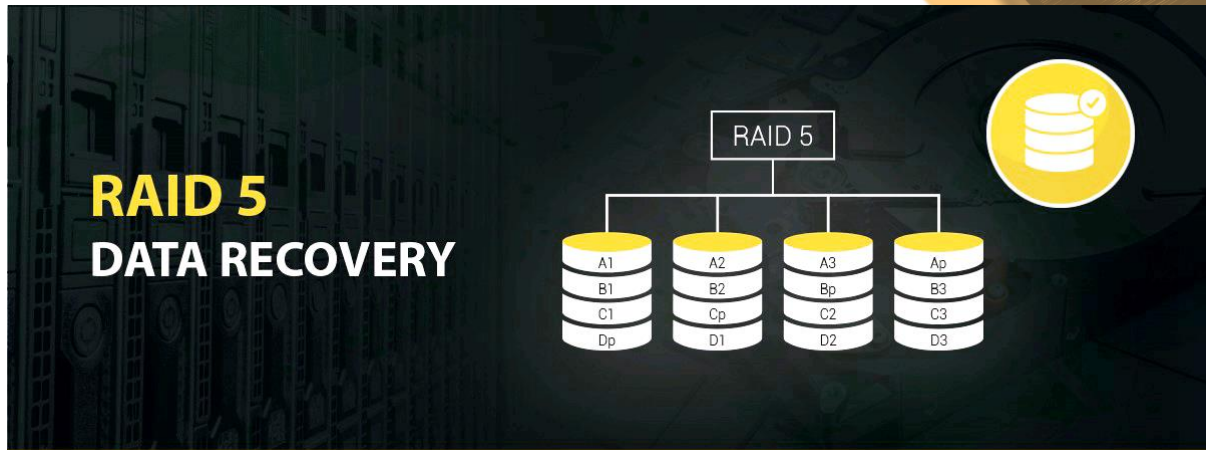
Dans le cas de l'adoption de la méthode de centralisation ou d'externalisation des données, afin d'anticiper tout risque concernant les données des différents utilisateurs, un système de gestion des droits sur les fichiers (Par utilisateur ou par service) devra être établi.

Enfin, une perte de données peut aussi subvenir en cas de coupure de courant ou de surtension entre autres. De fait, pour minimiser les risques liés à votre réseau électrique, la mise en place de systèmes de batteries de secours (Onduleurs), va vous permettre de maintenir votre réseau et donc, vos processus de sauvegarde des données.

La structure du réseau que nous recommandons se base donc sur l'architecture illustrée ci-dessous :



Par ailleurs, dans le cadre de la mise en place du serveur de stockage des données de la société, l'équipe d'ITS recommande fortement une installation basée sur l'architecture de stockage en RAID5 :



En effet, dans le cadre de cette architecture de serveur de stockage, vos données seront réparties sur chacun des disques qui constitueront le serveur via un système de parité.

Dans le cadre d'une telle configuration, notre objectif est de mettre en avant la sécurité de vos données en économisant leur volume de stockage.

Ainsi, en envisageant la défaillance d'un des disques de stockage du serveur, les données se retrouvent conservées et récupérables via les autres disques qui le constituent.

Bien entendu, une intervention sera nécessaire afin de remplacer le volume défaillant, mais aucune perte de données ne sera à encaisser par la société AutoConcept.



## V. NOS GARANTIES

NOTRE CHARTE QUALITE





# Informatics Safety

vous garantit

-  **S**ECURITE  
Respect et confidentialité des données ;  
Protection et sauvegarde des informations.
-  **A**CCOMPAGNEMENT  
Conseils organisationnels ou infrastructure réseau ;  
Formation aux droits et à l'utilisation de l'outil informatique.
-  **F**IABILITE  
Partenaire agréé Microsoft ;  
Certification ISO-9001.
-  **E**FFICACITE  
Réactivité et disponibilité, 24h/24, 7j/7 ;  
Contrôle qualité constant.





# Informatics Safety

exige que vous sachiez faire preuve d'

A

## ADAPTATION

Certains contacts ou interventions mettront votre vivacité d'esprit à l'épreuve. Soyez réactif et imaginatif !

D

## DISCRETION

Les données que vous pouvez consulter ne vous appartiennent pas, merci de veiller à ne pas les redistribuer.

A

## AMELIORATION

Nous ne doutons pas de vos compétences, mais l'informatique évolue constamment, vos compétences doivent donc faire de même.

P

## PRESENTATION

N'oubliez pas que la politesse et votre tenue sont les premières clés de votre réussite.

T

## TRANSPARENCE

Malgré les raccourcis employés en vertu de la pédagogie, ne manquez pas de développer le contenu de vos rapports.

E

## EDUCATION

Vous êtes un expert en informatique, mais ne négligez pas de vous faire comprendre par nos clients.

R

## RIGUEUR

Bien entendu, le respect de vos horaires et des procédures de travail représente le professionnel que vous êtes.

## VI. ANNEXES

### ANNEXE 1 : INVENTAIRE MATERIEL ET LOGICIEL AUTOCONCEPT



## InformaTics Safety

INVENTAIRE MATERIEL ET LOGICIEL	
SOCIETE	AUTOCONCEPT
ADRESSE	5 Boulevard de l'Europe, 21800 QUETIGNY
TELEPHONE	03 80 36 84 10
MAIL	contact@autoconcept.com
NOMBRE D'ORDINATEURS	70 - 80 postes
NOMBRE DE PERIPHERIQUES RESEAU	ND
TAILLE TOTALE DU RESEAU	ND

Logiciels système	Logiciels de production

Catégorie de l'appareil	Article	Modèle	Nombre
Imprimante / Copieur			
Ordinateur fixe			
Ordinateur portable			
Routeur			
Onduleur			
Total			

Je soussigné ..... en qualité de ..... de l'établissement  
AutoConcept atteste que les informations collectées dans le cadre d'une intervention de la société  
InformaTics Safety en son sein sont exactes.

Fait à ..... le .../.../.....

Signature

## ANNEXE 2 : CHARTE INFORMATIQUE TYPE



### Préambule :

La présente charte concerne les ressources informatiques, les services internet, de messagerie et téléphoniques de l'entreprise ....., ainsi que tout autre moyen de connexion à distance permettant d'accéder, via le réseau informatique, aux services de communication ou de traitement électronique interne ou externe. Il s'agit principalement des outils suivants : ordinateurs portables et fixes, tablettes tactiles, téléphones portables et fixes, imprimantes, logiciels.

Cette charte s'applique à l'ensemble du personnel de l'entreprise ainsi qu'aux stagiaires, intérimaires et salariés d'entreprises extérieures exécutant un travail au sein de l'entreprise.

Le cadre réglementaire de la sécurité de l'information est complexe. Chaque membre du personnel se doit de respecter les règles juridiques applicables, notamment en matière :

- de respect des règles déontologiques et professionnelles,
- de respect des procédures de travail,
- de respect de l'organisation et des règles de délégation,
- de communication d'informations,
- d'utilisation des moyens informatiques mis à sa disposition dans le cadre de sa fonction.

L'utilisation de l'informatique est encadrée par une législation très stricte visant à protéger d'une part les atteintes aux droits de la personne résultant de l'utilisation des fichiers ou traitements informatiques, d'autre part les atteintes aux systèmes de traitement automatisé de données.

Par ailleurs, le Code de la Propriété Intellectuelle protège le droit de propriété attaché aux logiciels et aux données (textes, images et sons).

Concernant internet, l'ensemble des règles juridiques existantes ont vocation à s'appliquer lors de son utilisation.

Il résulte, de l'application de ces dispositions légales, des règles internes qu'il est demandé à chacun de respecter :

### 1. Confidentialité de l'information et obligation de discrétion

Le personnel est soumis au secret professionnel. L'utilisateur doit assurer la confidentialité des données qu'il détient.

La création et l'utilisation de fichiers contenant des informations nominatives doivent faire l'objet d'une demande préalable auprès de la Commission Nationale Informatique et Liberté (C.N.I.L.).

Un comportement exemplaire est exigé dans toute communication orale ou écrite, téléphonique ou électronique, que ce soit lors d'échanges professionnels ou au cours de discussions relevant de la sphère privée.

L'accès par les utilisateurs aux informations et documents conservés sur les systèmes informatiques doit être limité à ceux qui leur sont propres, ainsi que ceux publics ou partagés. Il est ainsi interdit de prendre connaissance des informations détenues par d'autres utilisateurs, même si ceux-ci ne les



ont pas explicitement protégées. Cette règle s'applique en particulier aux données couvertes par le secret professionnel, ainsi qu'aux conversations privées de type courrier électronique dont l'utilisateur n'est ni directement destinataire, ni en copie.

L'utilisateur doit assurer la confidentialité des données qu'il détient. En particulier, il ne doit pas diffuser à des tiers, au moyen d'une messagerie non sécurisée, des informations nominatives et/ou confidentielles couvertes par le secret professionnel.

## *2. Protection de l'information*

Les documents bureautiques produits doivent être stockés sur des serveurs de fichiers.

Ces espaces sont à usage professionnel uniquement.

Le stockage de données privées sur des disques réseau est interdit.

Les médias de stockage amovibles (clefs USB, CD, disques durs, etc...) présentent des risques très forts vis-à-vis de la sécurité : risques importants de contamination par des programmes malveillants ou risque de perte de données. Leur usage doit donc être fait avec une très grande vigilance. L'entreprise se réserve le droit de limiter voire d'empêcher l'utilisation de ces médias en bloquant les ports de connexion des outils informatiques.

## *3. Usage des ressources informatiques*

Seules les personnes autorisées par la Direction ont le droit d'installer de nouveaux logiciels, de connecter de nouveaux PC au réseau de l'entreprise et plus globalement d'installer de nouveaux matériels informatiques.

Les matériels et logiciels informatiques sont réservés à un usage exclusivement professionnel et ne doivent pas être utilisés à des fins personnelles, sauf autorisation préalable de la Direction.

Conformément aux dispositions légales et réglementaires, il est également interdit à tout salarié de copier un logiciel informatique, d'utiliser un logiciel "piraté", et plus généralement, d'introduire au sein de l'entreprise un logiciel qui n'aurait pas fait l'objet d'un accord de licence. L'entreprise se réserve le droit de détruire le logiciel utilisé en violation de ces dispositions.

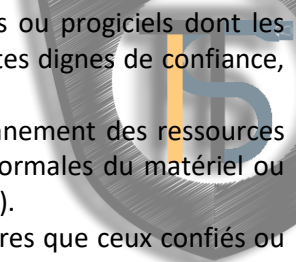
A l'exception des ordinateurs portables mis à la disposition des salariés, aucun matériel ni logiciel informatique appartenant à l'entreprise ne peut être sorti de celle-ci sans autorisation préalable de la Direction.

Lors de son départ définitif de l'entreprise, chacun est tenu de restituer les matériels, logiciels et documentations informatiques, qui lui auront été confiés en vue de l'exécution de son travail, et ce, en bon état.

Chaque utilisateur s'engage à :

- Ne pas modifier la configuration des ressources (matériel, réseaux, etc...) mise à sa disposition, sans avoir reçu l'accord préalable et l'aide des personnes habilitées dans l'entreprise.
- Ne pas faire de copies des logiciels commerciaux acquis par l'entreprise.



- 
- Ne pas installer, télécharger ou utiliser sur le matériel des logiciels ou progiciels dont les droits de licence n'ont pas été acquittés, ou ne provenant pas de sites dignes de confiance, et sans autorisation des personnes habilitées dans l'entreprise.
  - Ne pas apporter volontairement des perturbations au bon fonctionnement des ressources informatiques et des réseaux que ce soit par des manipulations anormales du matériel ou par l'introduction de logiciels parasites (virus, chevaux de Troie, etc...).
  - Ne pas connecter directement aux réseaux locaux des matériels autres que ceux confiés ou autorisés.
  - Informer immédiatement la Direction de toute perte, anomalie ou tentative de violation de ses codes d'accès personnels.
  - Effectuer une utilisation rationnelle et loyale des services et notamment du réseau, de la messagerie, des ressources informatiques, afin d'en éviter la saturation ou l'abus de leur usage à des fins personnelles.
  - Récupérer sur les matériels d'impression (imprimantes, télécopieurs) les documents sensibles envoyés, reçus, imprimés ou photocopiés.
  - Ne pas quitter son poste de travail en laissant accessible une session en cours et à ne pas se connecter sur plusieurs postes à la fois.

#### 4. *Respect du réseau informatique*

L'utilisation du réseau intranet doit se faire dans le respect des autres utilisateurs. Il est demandé à chacun de ne pas effectuer d'opérations qui pourraient avoir pour conséquence :

- d'interrompre ou de perturber le fonctionnement du réseau ou d'un système connecté au réseau ;
- d'accéder à des informations privées d'autres utilisateurs du réseau ;
- de modifier ou de détruire des informations sur un des systèmes connectés au réseau.

L'accès au réseau intranet est soumis à une identification préalable de l'utilisateur, qui dispose alors d'un "compte d'accès personnel" aux ressources et services multimédias.

Ce dernier est constitué d'un identifiant et d'un mot de passe strictement personnel et confidentiel. Leur usage ne peut en aucun cas être divulgué, transmis ou concédé à une autre personne.

L'utilisateur est responsable de son compte et de son mot de passe, et de l'usage qu'il en fait. Il ne doit pas masquer son identité sur le réseau local ou usurper l'identité d'autrui en s'appropriant le mot de passe d'un autre.

#### 5. *Usage des outils de communication*

L'entreprise tolère un usage exceptionnel, à des fins autres que professionnelles, des ordinateurs et des technologies de l'information et des communications, notamment internet et des courriers électroniques ne mettant pas en cause le temps de travail, n'affectant pas le bon fonctionnement et ne portant pas atteinte à l'intérêt collectif de l'entreprise.

Cette utilisation, à des fins personnelles, depuis le lieu de travail, est tolérée pendant les temps de pause ou pour des besoins urgents de la vie privée du salarié.

Elle doit être occasionnelle et raisonnable (tant dans la fréquence que dans la durée), conforme à la législation en vigueur et ne pas porter atteinte à la sécurité et à l'intégrité du système d'information ainsi qu'à l'image de marque de l'entreprise.

A l'exception des téléphones et tablettes portables mis à la disposition des salariés, aucun matériel de communication appartenant à l'entreprise ne peut être sorti de celle-ci sans autorisation préalable de la Direction.

Lors de son départ définitif de l'entreprise, chacun est tenu de restituer les téléphones, tablettes et autres outils de communication, qui lui auront été confiés en vue de l'exécution de son travail, et ce, en bon état.

- Accès à internet – navigation sur le WEB

Les données concernant l'utilisateur (sites consultés, messages échangés, etc...) peuvent être enregistrées par des tiers, analysées et utilisées à des fins notamment commerciale. Il est donc recommandé à chaque utilisateur de ne pas fournir son adresse électronique professionnelle, ni aucune coordonnée professionnelle sur internet, si ce n'est strictement nécessaire à la conduite de son activité professionnelle

L'utilisateur est informé que les traces de la navigation sont temporairement archivées. En effet, à la demande d'une autorité judiciaire ou administrative, l'administrateur du proxy devra fournir les informations de la navigation web.

L'entreprise se réserve le droit :

- de contrôler le contenu de toute page Web hébergée sur ses serveurs en vue de s'assurer du respect des conditions d'utilisation des services énoncées par la présente Charte.
- de suspendre l'usage du service d'hébergement des pages Web par un utilisateur en cas de non-respect de la Charte et notamment dans l'hypothèse où l'utilisateur aurait diffusé sur ses pages Web un contenu manifestement illicite.

L'utilisateur s'engage à respecter les règles suivantes :

- Interdiction de consulter ou télécharger du contenu de sites web à caractère pornographique, pédophile ou tout autre site illicite ou contraire aux bonnes mœurs.
- Interdiction de télécharger des fichiers musicaux ou vidéo.
- Pour participer à des forums, l'utilisateur doit disposer d'autorisations internes afin de s'exprimer au nom de l'entreprise.
- Les téléchargements de contenu illicite sont interdits (contrefaçon de marque, copie de logiciels commerciaux, etc...).

La consultation de sites web à titre privé est tolérée à titre exceptionnel et à condition que la navigation n'entrave pas l'accès professionnel et qu'elle s'effectue hors du temps de travail de l'utilisateur. La Direction se réserve le droit d'effectuer des contrôles sur les durées de connexion et les sites visités.

- Utilisation de la Messagerie électronique

La messagerie électronique permet de faciliter les échanges entre les salariés en interne.

Elle est réservée à un usage professionnel.

Il est interdit d'utiliser la messagerie électronique pour des correspondances sans lien direct avec l'activité professionnelle du salarié dans l'entreprise.

La réception d'une correspondance extra-professionnelle ne sera pas considérée comme fautive, dans la mesure où le salarié concerné, dès lors qu'il en aura pris connaissance, aura procédé sans délai à sa destruction.

Toutefois, l'inscription volontaire à une liste de diffusion sans lien avec l'activité professionnelle est interdite.

Il appartient à l'utilisateur d'identifier les messages qui sont personnels par la mention « personnel » ou « confidentiel » dans l'objet du message.

A défaut d'une identification, les messages sont présumés être professionnels. La Direction se réserve le droit d'effectuer des contrôles sur le nombre de messages échangés, la taille des messages échangés et le format des pièces jointes.

Afin de ne pas surcharger les serveurs de messagerie, il est attendu de chaque utilisateur, une gestion des messages (suppression, archivage, effacement périodique) et de la taille des pièces jointes envoyées.

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé à son responsable hiérarchique.

#### *6. Droit à la déconnexion*

Le droit à la déconnexion s'entend comme le droit de chaque salarié de ne pas répondre aux courriels et autres messages en dehors des heures de travail, afin de garantir l'équilibre entre vie professionnelle et vie privée, les temps de repos et de récupération, de réguler la charge mentale et réduire les risques de burn-out.

Le droit à la déconnexion dans l'entreprise fait l'objet d'un accord d'entreprise dans le cadre de la négociation annuelle sur l'égalité professionnelle entre les hommes et les femmes et la qualité de vie au travail.

La mise en œuvre du droit à la déconnexion dans l'entreprise passe notamment par :

- La mise en veille des serveurs informatiques en dehors des heures travaillées ;
- La programmation de pop-ups de sensibilisation lors de l'envoi d'un message pendant les temps de repos ;
- Une signature de courriel ou un message d'absence mentionnant ce droit ;
- Un cadrage managérial des salariés ne le respectant pas ;
- La sensibilisation et la formation à un usage raisonnable des outils numériques.

#### *7. Utilisation des outils numériques pour favoriser le droit d'expression*

Le droit d'expression directe et collective des salariés vise à définir les actions à mettre en œuvre pour améliorer l'organisation et les conditions de travail, ainsi que la qualité du travail réalisée au sein de l'équipe, du site ou de l'entreprise.

Les outils numériques disponibles dans l'entreprise peuvent être utilisés pour favoriser ce droit d'expression. Il en est ainsi notamment :

- des outils comme les réseaux sociaux de l'entreprise ou les forums ;
- pour des échanges en direct : des outils de visioconférence ou de messagerie instantanée avec vidéo ;
- d'autres modalités de recueil d'expression comme les baromètres sociaux.



## 8. Informatique et libertés

Un recours croissant à l'usage des technologies de l'information exige que chacun respecte les principes du droit à la protection des données personnelles dans ses deux volets : droits individuels et obligations.

Toute création ou modification de fichier comportant des données nominatives ou indirectement nominatives doit, préalablement à sa mise en œuvre, être déclarée auprès du Correspondant Informatique et libertés (C.I.L.) de l'entreprise, *Madame / Monsieur ..... (nom, prénom)*, qui étudie alors la pertinence des données recueillies, la finalité du fichier, les durées de conservation prévue, les destinataires des données, le moyen d'information des personnes fichées et les mesures de sécurité à déployer pour protéger les données. Le C.I.L. procède ensuite aux opérations de déclaration et d'information réglementaire.

Le C.I.L. permet de garantir la conformité de l'entreprise à la loi Informatique et Libertés.

Cette maîtrise des risques juridiques est d'autant plus importante que la plupart des manquements à la loi du 6 janvier 1978 sont pénalement sanctionnés.

En cas de non-respect des obligations relatives à la loi informatique et libertés, le C.I.L. sera informé et pourra prendre toutes mesures nécessaires pour mettre fin au traitement illégal ainsi qu'informer le responsable hiérarchique de l'utilisateur à l'origine du traitement illégal.

## 9. Surveillance du système d'information

- Contrôle:

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

L'utilisateur est informé que pour effectuer la maintenance corrective, curative ou évolutive, le personnel du service informatique dispose de la possibilité de réaliser des interventions (le cas échéant à distance) sur les ressources mises à sa disposition, et qu'une maintenance à distance est précédée d'une information de l'utilisateur.

Réseau intranet : L'entreprise peut vérifier à posteriori l'identité de l'utilisateur ayant accédé ou tenté d'accéder à une application au moyen du compte utilisé pour cet accès ou cette tentative d'accès.

Internet : L'entreprise dispose des moyens techniques suivants pour procéder à des contrôles de l'utilisation de ses services :

- Limites d'accès au serveur proxy ;
- Pare-feu.



L'entreprise garantit à l'utilisateur que seuls ces moyens de contrôle sont mis en œuvre.

Ces contrôles techniques peuvent être effectués :

- soit dans un souci de protection des mineurs (*en fonction de l'activité de l'entreprise*) ;
- soit dans un souci de sécurité du réseau et/ou des ressources informatiques.

Pour des nécessités de maintenance et de gestion technique, l'utilisation des services et notamment des ressources matérielles et logicielles, ainsi que des échanges via le réseau peuvent être analysés et contrôlés dans le respect de la législation applicable et notamment dans le respect des règles relatives à la protection de la vie privée et au respect des communications privées.

L'entreprise se réserve, dans ce cadre, le droit de recueillir et de conserver les informations nécessaires à la bonne marche du système. Elle se réserve la possibilité de procéder à un contrôle des sites visités afin d'éviter l'accès par ces derniers à des sites illicites ou requérant l'âge de la majorité.

- Traçabilité:

L'entreprise assure une traçabilité sur l'ensemble des accès aux applications et aux ressources informatiques qu'elle met à disposition pour des raisons d'exigence réglementaire de traçabilité, de prévention contre les attaques et de contrôle du bon usage des applications et des ressources.

Par conséquent, les applications de l'entreprise, ainsi que les réseaux, messagerie et accès internet intègrent des dispositifs de traçabilité permettant le contrôle si besoin de :

- L'identifiant de l'utilisateur ayant déclenché l'opération.
- L'heure de la connexion.
- Le logiciel ou programme utilisé.

Le personnel du service informatique respecte la confidentialité des données et des traces auxquelles il est amené à accéder dans l'exercice de ses fonctions, mais peut être amené à les utiliser pour mettre en évidence certaines infractions commises par les utilisateurs.

## 10. Alertes

Tout constat de vol de matériel ou de données, d'usurpation d'identité, de détournement de moyen, de réception de messages interdits, de fonctionnement anormal ou de façon plus générale toute suspicion d'atteinte à la sécurité ou manquement substantiel à cette charte doit être signalé à son responsable hiérarchique.

## 11. Responsabilités

L'attention du personnel est attirée sur le fait qu'en cas d'atteinte à un de ces principes protégés par la loi, la responsabilité pénale et civile de la personne, ainsi que celle de l'entreprise est susceptible d'être recherchée. (Articles 1383 et 1384 du Code Civil et Article 121-2 du Code Pénal)

L'utilisateur qui ne respectera pas les règles juridiques applicables, notamment celles rappelées ci-dessus, verra sa responsabilité juridique personnelle engagée non seulement par toute personne ayant subi un préjudice du fait du non-respect de ces règles, mais aussi de l'entreprise en sa qualité d'employeur.



L'entreprise ne pourra être tenue pour responsable des détériorations d'informations ou des infractions commises par un utilisateur qui ne se sera par conformé aux règles d'accès et d'usage des ressources informatiques et des services internet décrit dans la Charte.



#### 12. Date d'entrée en vigueur

La présente charte entre en vigueur le .....

Les règles définies dans la présente Charte ont été fixées par la Direction de l'entreprise dans le respect des dispositions législatives et réglementaires applicables et soumises à la consultation du Comité d'Entreprise *ou* de la Délégation Unique du Personnel *ou* des Délégués du Personnel.

La présente charte est portée, par tout moyen, à la connaissance des personnes ayant accès aux lieux de travail et aux locaux où se fait l'embauche.

Elle est également transmise en deux exemplaires à l'inspection du travail et au secrétariat greffe du conseil de prud'hommes de BELFORT.

Fait à ....., le .....

En 3 exemplaires originaux

Le Directeur

Nom / Prénom

Signature

## ANNEXE 3 : LEGISLATION ASSOCIEE



*L'article 1383 du Code Civil* prévoit que :

*« Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »*

*L'article 1384 du Code Civil* pose la responsabilité spécifique des employeurs du fait de leurs employés :

*« On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre [...] les maîtres et les commettants du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés »*

*L'article 121-2 du Code Pénal* prévoit la responsabilité des personnes morales responsables de leurs employés :

*« Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants.*

*La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3».*

*L'article 122-6-1 du Code de la Propriété Intellectuelle* prévoit les limites de l'exploitation logicielle et informatique comme suit :

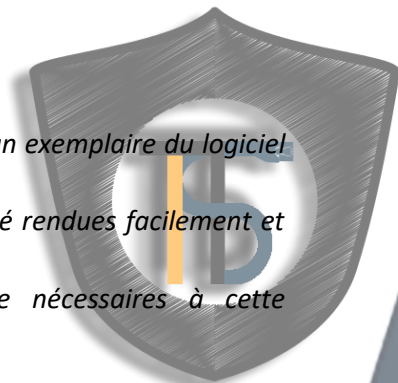
*« I. Les actes prévus aux 1° et 2° de l'article L. 122-6 ne sont pas soumis à l'autorisation de l'auteur lorsqu'ils sont nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser, y compris pour corriger des erreurs.*

*Toutefois, l'auteur est habilité à se réserver par contrat le droit de corriger les erreurs et de déterminer les modalités particulières auxquelles seront soumis les actes prévus aux 1° et 2° de l'article L. 122-6, nécessaires pour permettre l'utilisation du logiciel, conformément à sa destination, par la personne ayant le droit de l'utiliser.*

*II. La personne ayant le droit d'utiliser le logiciel peut faire une copie de sauvegarde lorsque celle-ci est nécessaire pour préserver l'utilisation du logiciel.*

*III. La personne ayant le droit d'utiliser le logiciel peut sans l'autorisation de l'auteur observer, étudier ou tester le fonctionnement ou la sécurité de ce logiciel afin de déterminer les idées et principes qui sont à la base de n'importe quel élément du logiciel lorsqu'elle effectue toute opération de chargement, d'affichage, d'exécution, de transmission ou de stockage du logiciel qu'elle est en droit d'effectuer.*

*IV. La reproduction du code du logiciel ou la traduction de la forme de ce code n'est pas soumise à l'autorisation de l'auteur lorsque la reproduction ou la traduction au sens du 1° ou du 2° de l'article L. 122-6 est indispensable pour obtenir les informations nécessaires à l'interopérabilité d'un logiciel créé de façon indépendante avec d'autres logiciels, sous réserve que soient réunies les conditions suivantes :*



*1° Ces actes sont accomplis par la personne ayant le droit d'utiliser un exemplaire du logiciel ou pour son compte par une personne habilitée à cette fin ;*

*2° Les informations nécessaires à l'interopérabilité n'ont pas déjà été rendues facilement et rapidement accessibles aux personnes mentionnées au 1° ci-dessus ;*

*3° Et ces actes sont limités aux parties du logiciel d'origine nécessaires à cette interopérabilité.*

*Les informations ainsi obtenues ne peuvent être :*

*1° Ni utilisées à des fins autres que la réalisation de l'interopérabilité du logiciel créé de façon indépendante ;*

*2° Ni communiquées à des tiers sauf si cela est nécessaire à l'interopérabilité du logiciel créé de façon indépendante ;*

*3° Ni utilisées pour la mise au point, la production ou la commercialisation d'un logiciel dont l'expression est substantiellement similaire ou pour tout autre acte portant atteinte au droit d'auteur.*

*V. Le présent article ne saurait être interprété comme permettant de porter atteinte à l'exploitation normale du logiciel ou de causer un préjudice injustifié aux intérêts légitimes de l'auteur.*

*Toute stipulation contraire aux dispositions prévues aux II, III et IV du présent article est nulle et non avenue. »*

## ANNEXE 4 : DISPOSITIF DE PREVENTION A LA SECURITE INFORMATIQUE



### Prérequis :

- Clé USB de 64Go
- Etiquetage de la clé USB avec la mention « Salaires <Nom de société> »
- Programme espion (Spybot) ayant pour but de détecter et enregistrer le réseau de l'entreprise ainsi que tous les fichiers que ce dernier englobe.

### Programme et objectifs de la mise en situation :

A l'arrivée de l'agent au sein de la société, ce dernier déposera négligemment la clé USB sur un des bureaux bénéficiant du plus grand taux de passage des différents salariés, cadre inclus.

L'objectif de cet « abandon » négligent est de faire en sorte qu'un des salariés de la société prenne possession de la clé USB et la consulte par la suite sur un des postes de la société. Cette dernière bénéficiant d'un parc informatique riche est particulièrement sensible à ce type de risque.

Suite à la connexion du périphérique USB à un des ordinateurs de la société, le programme inclus sur celle-ci va alors procéder aux actions suivantes :

- Copie du programme de la clé dans le système d'exploitation de l'ordinateur sur lequel est branchée la clé USB ;
- Détection du poste sur lequel est connectée la clé (Enregistrement de l'adresse IP de la machine) ;
- Lecture de l'architecture réseau, notamment via les ports 21, 80 et 110 depuis le poste infecté et enregistrement de celle-ci ;
- Lecture et archivage de la liste des fichiers contenus sur le poste ;
- Utilisation du routeur pour envoyer les informations sur l'appareil mobile de l'agent, qu'il pourra par la suite diffuser lors de la réunion avec le personnel de la société ;
- Réplication du programme sur les autres machines du réseau et répétition du cycle jusqu'à infection complète du réseau de la société.

*Bien entendu, une porte de sortie est incluse dans le programme inclus sur la clé, qui permet la suppression de l'« infection » sans que la moindre donnée soit conservée par nos agents. Ce programme a pour vocation de prévenir ce type de risques et non exposer la société s'engageant avec nous dans le cadre d'une information à la sécurité des données.*

## ANNEXE 5 : GLOSSAIRE



**Antivirus** : Un antivirus est un logiciel informatique destiné à identifier et à effacer des logiciels malveillants (malwares en anglais), également appelés virus, Chevaux de Troie ou vers selon les formes. Aujourd'hui, les logiciels antivirus sont fournis avec un pare-feu et parfois, un VPN.

**Architecture réseau** : Il s'agit de l'organisation des différents équipements informatiques permettant la transmission des données.

**Drivers (Pilotes)** : Ces derniers sont des programmes informatiques destinés à permettre à un autre programme (souvent un système d'exploitation) d'interagir avec un périphérique.

**Mastering (Matriçage)** : Le mastering est le processus qui consiste à transférer un ensemble de drivers, programmes et fichiers pour en faire un programme unique qui servira à une application en série de ce dernier.

**Onduleur** : L'onduleur est un dispositif permettant de protéger des matériels électroniques contre les surtensions ou bien les coupures de courant grâce à son système de bascule sur batterie interne. Il se présente souvent sous forme d'un boîtier placé entre le réseau électrique et les appareils à protéger.

**Pare-feu** : On parle ici d'un logiciel ou matériel permettant de faire respecter une politique de sécurité sur un réseau informatique. Ce dernier définit en effet quels sont les types de communications autorisées sur le réseau à travers de multiples règles.

**Programme propriétaire** : Il s'agit simplement d'un logiciel dont les droits ne sont pas libres mais encadrés par un contrat de licence utilisateur final (CLUF).

**RAID** : Le RAID est un ensemble de techniques de virtualisation du stockage de données qui permet de répartir des données sur plusieurs disques durs pour en améliorer les performances et/ou la sécurité à travers la tolérance aux pannes.

**Routeur** : Ce dernier est un élément intermédiaire dans un réseau informatique. Il assure la répartition des paquets (Connexion) selon un ensemble de règles définissables.

**Serveur** : Il s'agit d'un dispositif informatique matériel ou logiciel qui offre des services, généralement de stockage de données, à un ou plusieurs « clients ».

**VPN (Virtual Private Network)** : Ce système désigne un réseau chiffré dans le réseau Internet. Il sert principalement dans le cadre du partage de documents de manière sécurisée entre différents sites géographiques.



