Société SIE

PROJET SAS

Externalisation des prestations informatiques du concessionnaire AutoConcept

Claire CARON, Léonel DROUHARD, Sébastien SOMBRET

05/07/2019

Table des matières

Introduction

Notre entreprise SIE se présente dans le cadre de l'appel d'offre concernant l'externalisation de votre service de maintenance et support informatique.

L'outil informatique est devenu indispensable en milieu professionnel. Cependant, l'entreprise dépendante de ce support doit le maîtriser dans tous les aspects pouvant affecter sa performance, notamment :
- l'action technique (maintenance matérielle et logicielle, sauvegarde des données, politique de mots de passe),
- le comportement des acteurs (relation client, bonnes pratiques de confidentialité),
- le cadre économique et juridique (charte informatique, formation du personnel, outil de filtrage internet, *consultation interne des organismes représentatifs du personnel ?*),

Cette étude personnalisée débutera par une présentation succincte de la SIE et d'AutoConcept. Ensuite, notre expertise précisera les besoins motivant ce projet. Ce travail préliminaire permettra d'analyser les problématiques qui en découlent.
Nous conclurons cette entrevue par les moyens à mettre en œuvre qui satisferont au mieux votre demande. (<= besoin de mettre ce paragraphe ???)

Chapitre 1 : Présentation SIE (Solution Informatique Externalisée)

La SIE est une entreprise de services du numérique qui regroupe 16 collaborateurs. Son champ d'action couvre les PME de toute l'agglomération rémoise depuis 2005. Notre panel de prestation est basé sur une qualité de service contractuelle. Elle comprend notamment des interventions physiques et à distance, des solutions de sécurité, la mise en place et l'application des réglementations.

Aujourd'hui, nous accompagnons une vingtaine de structures, tous métiers confondus, dans le contrôle de leurs infrastructures numériques.

Solution **I**nformatique

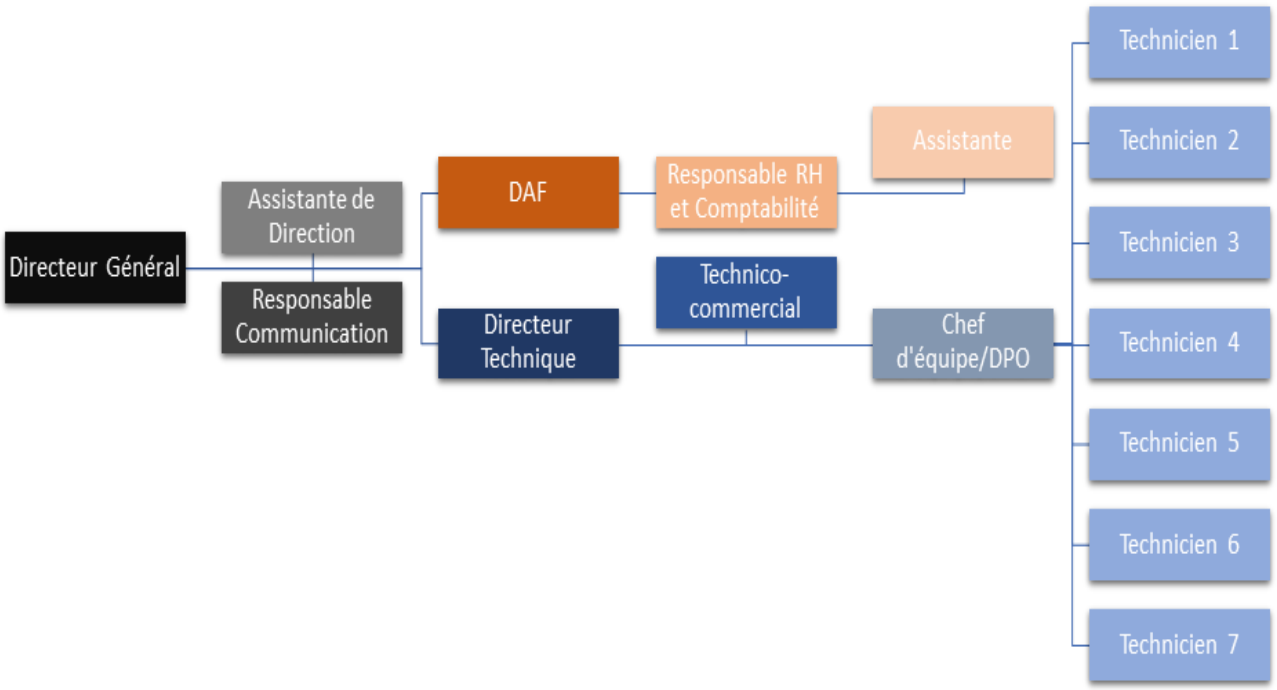
Externalisé

Tel :06.32.35.35.6

internet :

www.sie.fr

Siret :879 598 258
Siren
Chiffre d'affaire 125000


Directeur Général
Assistante de Direction
Responsable Communication
DAF
Directeur Technique
Responsable RH et Comptabilité
Technico-commercial
Assistante
Chef d'équipe/DPO
Technicien 1
Technicien 2
Technicien 3
Technicien 4
Technicien 5
Technicien 6
Technicien 7

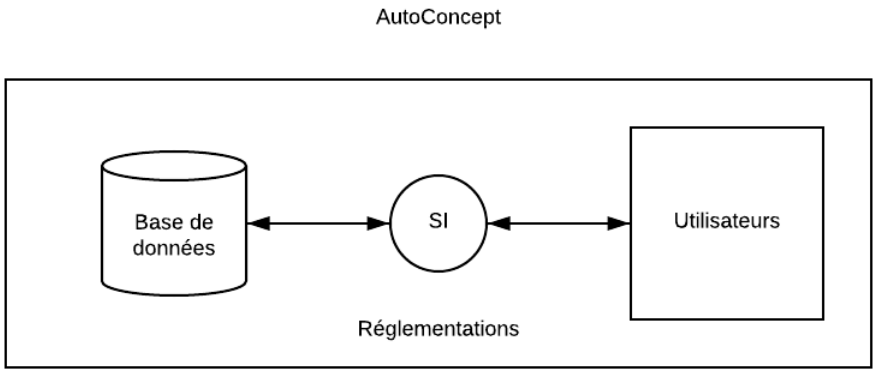
Chapitre 2 : Présentation AutoConcept

Vous êtes un concessionnaire automobile en activité à Reims et regroupant 83 collaborateurs. Environ 68 ordinateurs sont utilisés quotidiennement par le personnel. Deux salariés sont chargés de la gestion du parc numérique. Un de ces informaticiens sera recruté par le prestataire missionné. Par ailleurs, votre service commercial a communiqué le rapport de plaintes des utilisateurs PC.

Nous nous baserons donc sur ces éléments pour proposer un plan d'infogérance adapté à vos besoins.

Chapitre 3 : Reformulation des besoins

L'usage d'une infrastructure numérique se justifie dans une optique d'optimisation du traitement de l'information.



Les utilisateurs et la base de données représentent les deux environnements mis en relation par le système d'information (SI). Le cadre réglementaire fixe les limites au niveau de la loi, des bonnes pratiques relationnelles et informatiques.

Les besoins relevés dans les réclamations peuvent se présenter ainsi :

AutoConcept a besoin de :

Sauvegarder les fichiers sensibles ;
Améliorer l'accès à la base de données ;
Renforcer les mesures de confidentialité ;
Optimiser la communication entre tous les acteurs ;
Planifier l'ordre et la durée des opérations de maintenance ;
Former et informer le personnel sur l'utilisation de l'outil informatique ;
Standardiser les postes selon les services.

Pour aborder efficacement ces propositions, il sera pertinent de les hiérarchiser par services et par coefficient d'importance comme suit :

Besoins	Services AutoConcept						Coefficient	Total
	Atelier	Comptabilité	Véhicule Neuf	Véhicule Occasion	Pièce de rechange	Direction		
Sauvegarde								
Accès données								
Confidentialité								
Qualité relationnelle								
Planification maintenance								
Formation informatique au personnel								
Standardiser postes								

- Maintiens de la continuité de l'exploitation avec cinq machines prêtes à remplacer ;
- Remplacement des machines lentes par du neuf et transformation de ces machines en spare après reconditionnement ;
- Mise en place d'un serveur pour centraliser les sessions utilisateurs et un second pour les sauvegardes ;
- Filtrage des mails, Antivirus, Firewall*, et Gateway* ;
- Réponse et prise du problème d'un technicien 2h
- Suivis du ticket et enquête de satisfaction

- Suivis et changement du parc (propriétaire),
- 68 postes de travail actuellement propriétaires pour 83 membres du personnel ;
- Diagnostique des postes de travail actuels, ne changer que le nécessaire en attendant le renouvellement complet du parc ;

 Prise en charge et suivis de l'un des deux techniciens.

Chapitre 4 : Analyse des problématiques

Chaque problème traité ici représente un besoin non satisfait.

1. Sauvegarde

La politique de sauvegarde décide de l'avenir d'une entreprise qui en dépend. En cas d'insuffisance dans cette démarche, des données corrompues sont souvent irrécupérables. Les pertes d'exploitation sont alors à déplorer.

2. Exploitation de l'outil informatique

Un ordinateur devient le maillon faible d'une chaîne de traitement quand son utilisateur attend l'exécution d'une commande. Cette lenteur est généralement multifactorielle : disque dur, infection virale, poussière, optimisation logicielle… Il en résulte une productivité réduite et un agacement des utilisateurs.

3. Confidentialité

Il est à craindre, dans cette thématique, les accès non autorisés à des données sensibles. Pouvant survenir par manque de vigilance du personnel ou par les failles de sécurité du système informatique, la disponibilité excessive de ces informations provoque des fuites d'informations néfastes. Celles-ci concernent le domaine concurrentiel et les préjudices sur les données personnelles.

4. Qualité relationnelle

Le manque de pédagogie provoque l'incompréhension, qu'elle provienne du support technique ou des utilisateurs. L'incorrection dans le langage et la tenue sont, bien entendu, à proscrire. Éviter ces communications dégradées renforcera le bien-être du personnel et l'image positive de l'entreprise en présence du client.

5. Planification de la maintenance

Des utilisateurs laissés pour compte et les plannings non respectés sans justification sont contraires aux bonnes pratiques du technicien de maintenance. Les absences de retour, le dépassement des délais et les pannes redondantes augmentent la fréquence des réclamations, des retards et une baisse de confiance envers le support technique.

6. Formation numérique pour le personnel

Les bonnes pratiques informatiques ne concernent pas uniquement les informaticiens. Tous les services d'une entreprise devront exploiter, avec prudence et mesure, les postes à leur disposition. D'où l'importance d'avertir le personnel sur les répercussions d'usages non professionnels ou de négligence sécuritaire. Cette sensibilisation ciblera les demandes excessives des usages, ainsi que les sessions « trop » accessibles. (voir charte informatique et confidentialité)

Chapitre 5 : Analyse des Solutions et préconisation

Les problèmes étant identifiés, faisons la relation avec des objectifs réalistes.

1. Créer des supports de restauration

Un plan de sécurité efficace consiste en la multiplication du nombre de sauvegarde et leurs emplacements géographiques. Cela réduit grandement l'influence des données corrompues, de l'erreur humaine, des accidents et donc les pertes d'exploitations.

2. Augmenter la réactivité du système d'information

Le système d'information (serveur) au profit d'une gestion réseau s'appuyant sur la technologie SSD* améliore considérablement la fluidité des terminaux. Cette augmentation entraîne en même temps le rendement et la satisfaction des utilisateurs. À noter également que cette technologie subit moins de pannes. En outre, les déploiements via réseau réduisent fortement la durée des arrêts d'activités. Standardisation des postes. Uniformiser les postes de travail pour permettre un déploiement plus aisé et plus rapide sur des clients légers.

3. Restreindre l'accès aux données sensibles

Une politique de confidentialité s'établit via un contrat. Ce dernier régit le comportement des acteurs vis-à-vis d'informations confidentielles. Ainsi la rétention et le choix de ces fichiers critiques protègent l'entreprise, son personnel, ses clients. Le cadre légal servira de socle à cette initiative.

4. Améliorer la qualité des échanges

Le bien-être collectif fait tout autant l'objet d'un contrat. Le règlement intérieur précise les limites ; la note de service les remet en mémoire. Empêcher les attitudes néfastes réduit le stress des employés et bénéficie à l'image de la société.

5. Amplifier la communication du support technique

Échanger verbalement est insuffisant lorsqu'un technicien veille sur 40 postes. Il est alors nécessaire d'établir une plateforme de suivi efficiente. L'informaticien exploitant cette ressource est capable de hiérarchiser les demandes, d'y répondre, d'avertir, de documenter ses interventions. La démarche ITIL* est, à ce titre, une excellente base méthodologique.

6. Sensibiliser sur les bonnes pratiques numériques

La prévention en matière informatique est essentielle pour limiter les usages personnels abusifs. À cette fin, un filtrage mesuré des contenus permet le contrôle du trafic Internet (en plus de bloquer des intrusions). En outre, responsabiliser les utilisateurs accentue leur prise de conscience, non seulement des dangers du Web, mais aussi de l'impact des pratiques chronophages en entreprise. (voir charte informatique)

7. Préconisation

Un fichier en unique exemplaire est irremplaçable en cas de perte. Pourtant, la bonne santé d'une entreprise dépend essentiellement de sa documentation interne.

D'après une étude de IT Globale : « 80% des entreprises ayant perdu leurs données informatiques font faillite dans les 12 mois ».

D'après Ontrack : « 93% des entreprises qui ont perdu leurs données pendant 10 jours ont fait faillite dans l'année qui a suivi la perte ».

Ces chiffres sont à prendre avec des pincettes mais l'enjeu est bien réel.

Une fois le système de sauvegarde en fonction. Quand ces espaces de stockages seront intégrés dans les postes de travail, il nous suffira de déployer ladite sauvegarde sur le réseau de l'entreprise. Cette possibilité nous dispensera d'une installation individuelle sur chaque machine, bien plus chronophage.

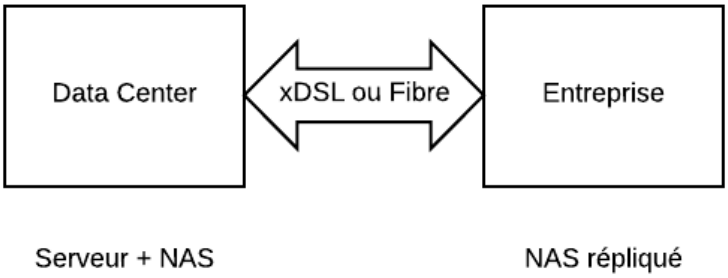
Le rendement d'une sauvegarde est difficilement mesurable. Il serait tout de même intéressant mettre en rapport le coût engendré par cette prestation et les pertes d'exploitation qu'elle pourrait éviter.

Par conséquent, nous recommandons la mise en place d'un système de sauvegarde comme premier objectif de votre externalisation. Une solution 3.2.1 trois sauvegardes sur deux supports diffèrent dont une en externe.

Mesures immédiates de sauvegardes

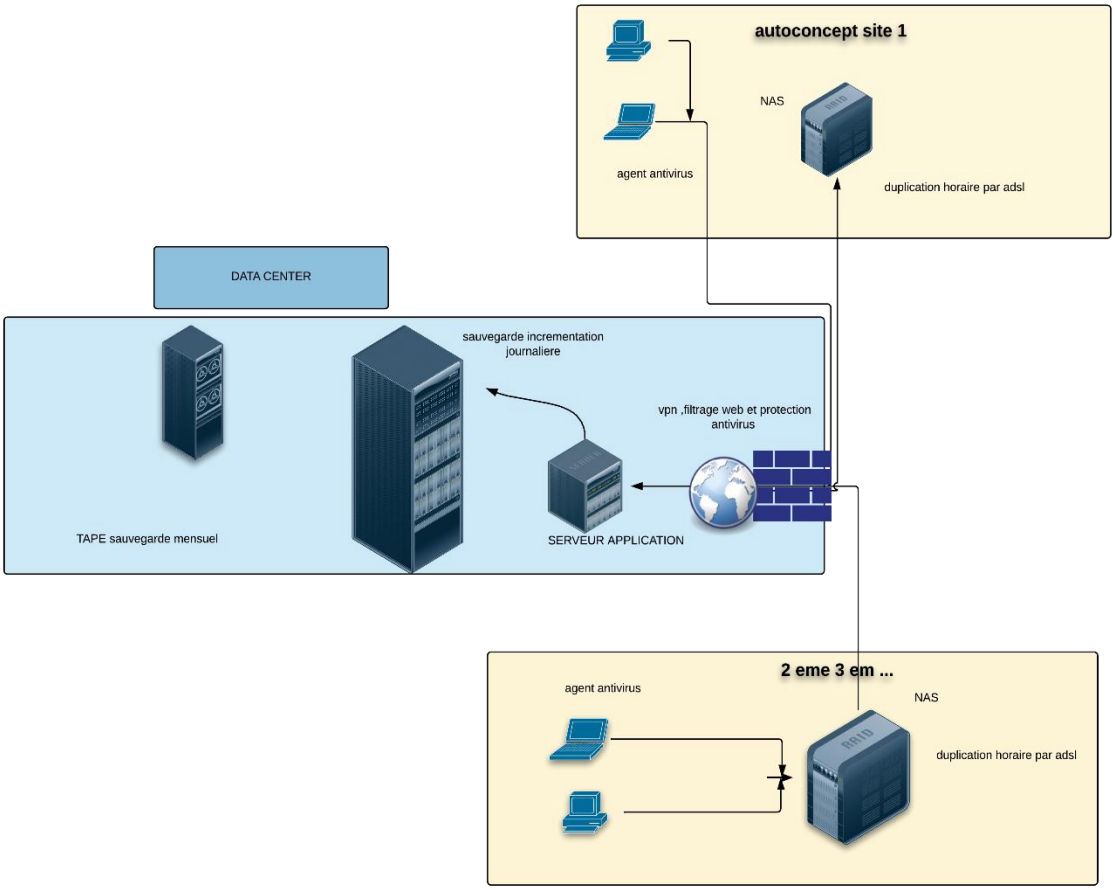
Dans un premier temps, créer un fichier partagé pour récupérer le travail des ordinateurs puis sauvegarder tout cela sur un NAS* pour mettre en place une sauvegarde automatisée sur votre site et synchronisée dans le Data Center*.
Dans un deuxième temps, création d'un serveur qui stockera toute vos sessions, également dans le Data Center.
Un nombre de postes supplémentaires en vue de dépanner rapidement un poste défaillant sans perte puisque tout sera stocker dans le serveur et sauvegardé sur un NAS sur votre site et un autre dans le Data Center.

8. Schéma de l'infrastructure



L'intérêt de ce dispositif se pose ainsi :

- L'équipe d'intervention spécialisée du Data Center sera sur place en cas de problème touchant le serveur et/ou le NAS attenant.
- La qualité des locaux du Data Center garantit une protection optimale contre les dommages matériels (incendie, explosion…) et les intrusions (vidéosurveillance, care d'accès…)


autoconcept site 1
NAS
agent antivirus
duplication horaire par adsl
DATA CENTER
sauvegarde incrementation journaliere
vpn ,filtrage web et protection antivirus
TAPE sauvegarde mensuel
SERVEUR APPLICATION
2 eme 3 em ...
agent antivirus
NAS
duplication horaire par adsl

Stratégie de sauvegarde

D'après les réclamations du personnel, une indisponibilité des données durant 2 jours suffit à provoquer des pertes d'exploitation. Sur cet exemple, un RPO* de 24h limitera les dégâts.

Le RTO* doit être inférieur au RPO pour éviter au maximum les pertes d'exploitation. En supposant le cas extrême, en termes de quantité de données perdues, pour une journée standard de travail :

Point de sauvegarde à 23h tous les jours et perte du service en fin de journée 18h.

Toutes les données de la journée seront perdues (seuil de tolérance). Une restauration dans la nuit pour rétablir le parc informatique serait idéale pour éviter la moindre interruption d'activité :

Incident déclaré en fin de journée 18h et restauration effective avant la reprise de l'activité le lendemain matin 8h.

Un RTO de 12 heures limitera la perte d'exploitation à une journée de travail.

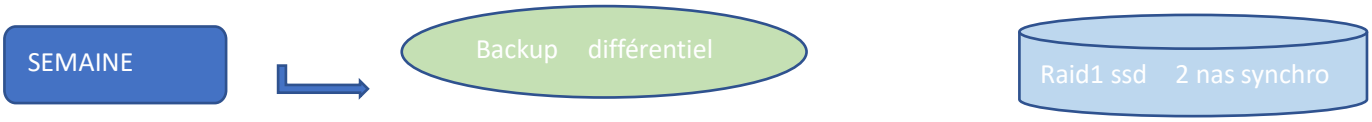
problème sur	ticket et prise en compte technicien	moyen	comment	resolution
poste de travail	2h max	spare en stock	remplacement de la machine par le technicien local	12h
souris	2h max	consomable en stock	en stock sur site	12h
un fichier excel	2h max	sauvegarde j-1	restauration de la sauvegarde j-1	12h
serveur ssd	2h max	spare ssd en stock	technicien sie , remplacement du disque	24 h

Planning de sauvegarde

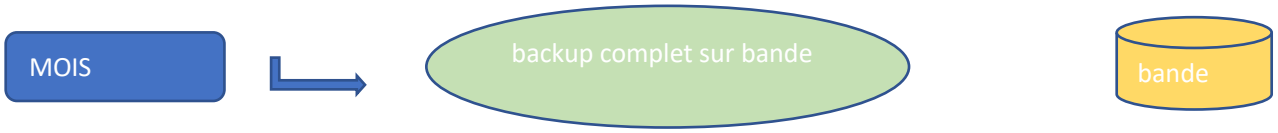
Une sauvegarde journalière, hebdomadaire et mensuelle réduira les risques de pertes, il sera possible de restaurer les données à :

- J-1, J-2, J-3, J-4, J-5, J-6, J-7 : sauvegarde incrémentale*;
- J-14, J-28, M-1, M-2, …, M-12 : sauvegarde différentielle*.

Une sauvegarde tous les jours à minuit à deux endroits différents.



Toutes les semaines un différentiel des fichiers est sauvegardé.



Tous les mois sont sauvegardés sur bande magnétique.

Une fois l'année en rétention révolue, la bande contenant l'année de sauvegarde sera archivée.

Conclusion

Une externalisation est guidée par l'équilibre entre l'importance des services et les ressources sollicitées. C'est sur cet équilibre que notre démarche se focalise. Nous espérons que cette étude vous sera profitable.

Et si cela vous "SIE" n'hésitez pas à nous contacter !

Annexes

° plan de sécurisation des données -

- Politique des mots de passe

Pour protéger vos informations, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.
Voici quelques recommandations :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc, ...) ;
- Ne demandez jamais à un tiers de générer 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 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.

La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document « Recommandations de sécurité relatives aux mots de passe ».

Si vous souhaitez une règle simple : choisissez des mots de passe d'au moins 8 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).

Blocage au bout de 3 tentatives échouées

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

« source Gouvernement guide mot de passe"

- Antivirus sur les postes de travail et serveur

- Filtrage internet un firewall avec une connexion vpn

CHARTE INFORMATIQUE SIE

CHARTE DU BON USAGE DES RESSOURCES INFORMATIQUES ET DU RESEAU DE SIE

Ladite charte, associée au règlement intérieur SIE, 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.

1. Définitions

On désignera de façon générale sous le terme « ressources informatiques », les moyens informatiques de gestion local ainsi que ceux auxquels il est possible d'accéder à distance,
Directement ou en cascade à partir du réseau administré par SIE.
On désignera par « services internet », 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.

À ce titre, la présente charte doit être communiquée à tout utilisateur interne ou extérieur à SIE 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 SIE et tout tiers donnant accès aux données, aux programmes informatiques ou à tout autre moyen de SIE 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, les hébergements externes et tout autre local de SIE disposant de tels matériels.
Les installations de SIE permettant de se connecter à 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. L'utilisation des ressources informatiques partagées de SIE 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 de SIE. 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.

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 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 de SIE;
- De ne pas respecter 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.
- Ne pas porter atteinte à l'intégrité, à l'image et à l'intérêt d'un autre utilisateur et/ou de SI, 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 de SIE, 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 encourageant 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 guerres et/ou contre l'humanité.

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

3.2. 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).

3.3. 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.
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.

3.4. 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 microordinateurs de SIE 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 de SIE (pour les postes dont SIE 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 de SIE.
En cas d'altérations des sanctions sont prévues.
Les actes consistant à empêcher le fonctionnement d'une ou des ressources informatiques de SIE, par exemple par l'introduction de virus ou par l'introduction ou la modification frauduleuse de données, sont répréhensibles.

3.5. 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.

- Contrevenir aux lois sur la propriété intellectuelle, littéraire et artistique ;
- Faire l'apologie de tout type de crime ou délit (racisme, antisémitisme, etc.).

4. Accès aux ressources informatiques

Le droit d'accès est limité à des activités conformes aux missions de SIE, notamment :
● 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 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 de SIE 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

Politique des mots de passe

Pour protéger vos informations, il est nécessaire de choisir et d'utiliser des mots de passe robustes, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés et à deviner par une tierce personne.
Voici quelques recommandations :

- Utilisez un mot de passe unique pour chaque service. En particulier, l'utilisation d'un même mot de passe entre sa messagerie professionnelle et sa messagerie personnelle est impérativement à proscrire ;
- Choisissez un mot de passe qui n'a pas de lien avec vous (mot de passe composé d'un nom de société, d'une date de naissance, etc, ...) ;
- Ne demandez jamais à un tiers de générer 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 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.

- La robustesse d'un mot de passe dépend en général d'abord de sa complexité, mais également de divers autres paramètres, expliqués en détail dans le document « Recommandations de sécurité relatives aux mots de passe ».
- Choisissez des mots de passe d'au moins 8 caractères de types différents (majuscules, minuscules, chiffres, caractères spéciaux).
- Blocage au bout de 3 tentatives échouées

Deux méthodes pour choisir vos mots de passe :

- La méthode phonétique : « J'ai acheté huit cd pour cent euros cet après-midi » deviendra ght8CD%E7am ;
- La méthode des premières lettres : la citation « un tien vaut mieux que deux tu l'auras » donnera 1tvmQ2tl'A.

● 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 de SIE 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 ;

● Assurer la protection de ses informations (l'utilisateur est responsable des droits qu'il donne aux autres utilisateurs)

● Signaler aux administrateurs systèmes 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 de SIE et plus particulièrement à l'intégrité et à la conservation des données de SIE.

● Ne pas utiliser les ressources informatiques de SIE à des fins de harcèlement, menace ou injure, et, de manière générale, violer les droits en vigueur

● Ne pas détourner des informations propres à SIE à des fins de concurrence déloyale, d'émettre de fausses déclarations visant à falsifier les données de SIE, de supprimer ou de modifier des données au préjudice de SIE ;

● Protéger ses ressources informatiques privées d'un antivirus récent et avec la dernière mise à jour.

5.2. Des administrateurs des systèmes informatiques

Les administrateurs des ressources informatiques de SIE 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 de SIE 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 constituants ou s'apparentant à des virus.

5.4. Utilisation des ressources informatiques

Chaque utilisateur s'engage à prendre soin du matériel 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.

5.5. Gestion des boîtes aux lettres électroniques

Tout utilisateur s'engage à utiliser le service pour un usage professionnel 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.

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

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 de SIE.

5.9. Les pare-feu / firewall

Les pares-feux vérifient tout le trafic sortant de SIE, 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

Les fichiers de journaux de traces 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.

7. 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 SIE induit l'acceptation sans réserve 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 réserve de la part de l'utilisateur.

8. Durée de validité et révision de la charte

SIE réserve le droit, à sa seule discrétion et sans information préalable, de modifier, supprimer ou ajouter des clauses à 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 SIE 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)

Sources : CESI

Charte Qualité SIE

Nous nous engageons à fournir un service de qualité à nos clients.

Transparence des actions à effectuer : SIE met en place un échange clair, à l'oral comme à l'écrit.

Écouter et répondre aux demandes/réclamations : SIE veille à ce que toutes les questions soient abordées.

Disponibilité : SIE délivre ses prestations tous les jours, à toute heure.

Viser une relation durable : SIE mise sur le partenariat à long terme pour répondre aux besoins toujours plus efficacement.

Respect dans les échanges : C'est dans la politesse et la considération que SIE s'adresse à chacun de ses clients.

Suivi de satisfaction personnalisé : Après chaque intervention, SIE se met à disposition pour recueillir les suggestions et améliorer sa qualité de service.

Solutions adaptées : SIE porte attention aux ressources sollicitées pour les utiliser de façon optimale.

Neutralité fournisseurs : SIE n'a pas de contrat privilégié avec ses fournisseurs. SIE se pose comme conseil auprès du client, et non comme intermédiaire (sauf sur demande).

Réactivité : SIE agit dès que possible grâce à un intervenant dédié à votre entreprise.

Garantie de résultat : SIE garantie ses prestations 14 jours après la reconnaissance de satisfaction.

Suivi des réparations : SIE s'engage à informer, de manière continue, l'évolution d'un dépannage via courriel, téléphone ou plateforme support.

Confidentialité des données : Chaque contrat du SIE comporte une clause de confidentialité en harmonie avec le règlement européen.

Soin des matériels, logiciels et données : SIE conserve l'intégrité des éléments que ses agents manipulent.

Compétences techniques : SIE regroupe une équipe d'intervenants qualifiés et d'un réseau de spécialistes afin de définir les meilleures solutions.

SIE met un point d'honneur à respecter toutes les conditions de ses engagements.

Charte de confidentialité

Depuis 15 ans, SIE a établi une relation de confiance avec chacun de ses clients. Elle est le fruit d'un engagement de chacun de ses collaborateurs et d'un très faible turnover du personnel.

Le piratage informatique devient un fléau qui touche tout le monde. Plusieurs cas de piratage sont effectués par des professionnels de l'informatique qui ont trouvé un moyen simple de réaliser des profits bien plus importants que ceux engendrés par des prestations d'installation et de SAV.

Le marché d'achat des informations (login/mot de passe, informations bancaires, négociation, vie privée, fichiers clients et collaborateurs, etc.) est fleurissant sur le « darknet ». Par exemple une simple adresse email avec ses logins et mots de passe se revend 25 USD. Une copie de disque dur complet 50 USD minimum. La demande est aujourd'hui extrêmement forte. Une adresse mise sur le marché se revend des dizaines de fois en quelques minutes.

La majorité des dirigeants ne réalise pas l'impact que pourrait avoir une personne mal intentionnée qui consulterait sa messagerie personnelle ou celles de son entreprise à son insu, pendant plusieurs mois. Il y a fort à parier que le pirate aurait connaissance des numéros de cartes, de la politique de mot de passe, des conditions commerciales et de nombreuses informations que le propriétaire de la boite mail ne souhaite pas voir exploitées par un tiers.

Ceci est un exemple, les risques de fuites et de destruction des données sont multiples (vandalisme interne et externe, intrusion réseau, etc, ...).

La direction de SIE est très vigilante sur le sujet de la confidentialité et de la protection de vos données et a mis en œuvre une série de procédures afin de garantir votre protection.

- Tous nos collaborateurs susceptibles d'avoir accès à vos données sont engagés contractuellement à la plus stricte confidentialité par contrat de travail et signature de notre annexe au règlement intérieur. Tout manquement à ces règles serait considéré comme une faute lourde et ferait appel aux autorités judiciaires.

- Tous nos techniciens, ingénieurs, chefs de projet et formateurs avant-vente sont en CDI. Ils sont engagés en fonction de leurs qualités techniques mais aussi morales.

- Nos collaborateurs sont régulièrement formés aux risques et dangers liés aux piratages informatiques ainsi qu'aux méthodes de protection.
- Chaque mois, une réunion entre nos techniciens est organisée afin d'échanger sur le sujet de la sécurité clients et nos procédures.

- SIE s'engage à ne jamais confier une intervention sur votre système informatique à un stagiaire ou toute autre personne non employée ou n'ayant pas signé notre règlement intérieur.

- Toute action, conseil ou préconisation de nos techniciens et commerciaux prendra en compte, en premier lieu, la protection et la confidentialité de vos données.

- SIE et son personnel s'engage à ne jamais réaliser de profit par l'exploitation de vos informations et/ou données.

- En cas de stockage temporaire de vos données par nos services pour des raisons techniques, nos collaborateurs s'engagent à vous en informer et à prendre toutes les dispositions pour les protéger.

1. En cas de dépannage, le technicien procèdera à une sauvegarde avant toute manipulation (sauf indication contraire du client).

2. En cas de dépannage en atelier le technicien s'engage à protéger l'accès à vos informations.

- Les logins et mots de passe administrateurs de vos serveurs seront confiés uniquement à la direction de nos clients, charge à eux de les divulguer ou non à leurs collaborateurs.

- SIE s'engage à ne jamais détenir et/ou modifier un mot de passe sans en informer et sans l'avoir préalablement confié à la direction.

- Aucune information sur les accès à vos serveurs ne sera donnée à un de vos collaborateurs sans une demande écrite de la direction. Il en va de même pour le paramétrage de boites email d'entreprise sur des terminaux nomades.

- Nos techniciens s'engagent à ne jamais divulguer aucune information de nos clients.

- Si l'un de nos techniciens remarque des manipulations douteuses d'origine interne ou externe, celui-ci s'engage à en informer la direction.

- Les accès internet et/ou wifi seront par défaut sécurisés par nos services (le choix des matériels proposé par SIE aura, avant toute autre caractéristique, été choisi par sa capacité à assurer une protection adaptée).

SIE s'engage sur simple demande du client à l'informer en toute objectivité sur :

- Les risques et les méthodes de protection de son infrastructure.

- Les avantages et inconvénients du Cloud, du big data et autres nouvelles technologies liées aux stockages et à la confidentialité des données.

- Les risques et les méthodes de protection contre la fuite des données.
- L'usage d'internet et de la messagerie dans l'entreprise.

- Les obligations des entreprises sur l'usage informatique (CNIL, etc, ...).

- Les documents importants à mettre en place dans l'entreprise (Annexe règlement intérieur, etc, ...).

Toutes ces formations seront effectuées gratuitement par SIE.

3. En cas de renvoi du matériel chez le constructeur, les données seront copiées et cryptées sur un support externe. Ledit support sera stocké dans un endroit sécurisé (alarme, vidéosurveillance, (coffre-fort sur demande)).

De plus, le matériel envoyé au constructeur sera vide de ses données (si la panne le permet). Nos techniciens s'engagent également à détruire les sauvegardes réalisées dès retour du matériel chez son propriétaire.

Mémo

<u>À l'attention de</u> :

Diffusion générale

Note de service n° 067/2019 du 1er juillet 2019

Objet : attitude à adopter face aux clients

<u>Tenue vestimentaire</u>

Chacun des membres du personnel est invité à adopter un code vestimentaire éthique approprié à l'exercice de son travail.

En ce sens, la tenue vestimentaire doit être empreinte de respect et de professionnalisme envers les clients, notamment lors des déplacements à l'extérieur. Les techniciens se verront fournir une tenue de travail adaptée et facilement identifiable.

<u>Consommation</u>

Au regard des exigences en matière de sécurité et de maîtrise du comportement inhérent à l'activité de l'entreprise, la consommation et l'introduction de boissons alcoolisées sur les lieux de travail sont strictement interdites.

Compte tenu des articles L. 3421-1 du Code de la Santé Publique et 222-37 du Code Pénal, la détention et l'usage de stupéfiants sont formellement prohibés. En conséquence, leur usage et leur introduction dans l'entreprise sont interdits.

L'arrivée sur les lieux de travail en état d'imprégnation de boissons alcoolisées et/ou de drogue, du fait d'une consommation en dehors de l'entreprise est également interdite.

Tout manquement à l'une de ces obligations est de nature à justifier une sanction disciplinaire.

Discrétion

Le personnel est tenu à une obligation de discrétion professionnelle concernant toutes les informations portées à sa connaissance dans l'exercice de ses fonctions et dont la divulgation pourrait nuire aux intérêts de l'entreprise, de nos clients, de nos fournisseurs ainsi que de nos partenaires commerciaux.

Il est également interdit de divulguer ces informations tant à l'intérieur qu'à l'extérieur de l'entreprise (clients, fournisseurs, concurrents…).

Comportement à l'égard des clients

L'image de marque de notre société est véhiculée par nos employés lors de leurs missions en extérieur ainsi que par la qualité de notre accueil et de nos prestations.

Il vous est donc demandé de bien vouloir adopter l'attitude adéquate face aux différentes situations (accueil client, helpdesk, prospection commerciale…).

La ponctualité et l'amabilité sont primordiales tout comme le sourire, ils renvoient une image positive de l'entreprise.

Communication

Dans un souci de transparence, il est demandé aux techniciens de communiquer avec leur hiérarchie sur l'état d'avancement des interventions par le biais du reporting ainsi qu'avec les clients via la gestion de tickets.

Vous devrez informer les clients en employant la vulgarisation des termes dits « trop techniques ».

Satisfaction client

Une ouverture de ticket sera suivie d'un questionnaire afin de mesurer le degré de satisfaction de l'utilisateur après une intervention.

Le Directeur Général

Note de synthèse sur l'aspect juridique

La CNIL* est l'autorité administrative chargée de l'application des règlementations concernant les usages du numérique. « Elle a un rôle d'alerte, de conseil et d'information vers tous les publics mais dispose également d'un pouvoir de contrôle et de sanction. »
Le RGPD* n° 2016/679 du 27 avril 2016 fédère les états européens autour d'un cadre légal commun, portant sur le traitement des données à caractère personnel.
Nous utiliserons ces références pour aborder les points suivants :

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

Le RGPD est un socle incontournable de la majorité des entreprises européennes. Toutes celles manipulant des données, telles que le nom, l'âge, l'adresse d'un client, sont concernées. Selon les recommandations de la CNIL, 6 étapes doivent s'articuler successivement :

- Désigner un pilote ;
- Cartographier les traitements de données personnelles (sauvegarde, correctifs, …) ;
- Prioriser les actions à mener ;
- Gérer les risques ;
- Organiser les processus internes (demandes d'accès, durée de rétention, anticipation des violations de données, …) ;
- Documenter la conformité.

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

La CNIL fournit également une documentation en ligne, faisant écho au RGPD. Ce guide de la sécurité des données personnelles traite 17 points parmi lesquels :

- Sensibiliser les utilisateurs ;
- Authentifier les utilisateurs ;
- Gérer les habilitations ;
- Etc.

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

« Les salariés doivent être informés :

- Des finalités poursuivies ;
- De la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur) ;
- Des destinataires des données ;
- De leur droit d'opposition pour motif légitime ;
- De la durée de conservation des données ;
- De leurs droits d'accès et de rectification ;

- La possibilité d'introduire une réclamation auprès de la CNIL. »

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

Avant l'entrée en application du RGPD, une déclaration à la CNIL était obligatoire pour l'instauration de filtrages des contenus abusifs. Cette démarche n'est plus nécessaire mais l'entreprise voit sa responsabilité accrue. Elle s'assurera de déployer ces contrôles uniquement pour :

- « Assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de Troie, etc.) ;
- Limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de sa messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux, etc, ...). »

Spare

- Une gestion dédiée client qui permet une réactivité optimale ;
- Un outil de gestion des stocks avec GLPI ;
- Un stock tampon de matériel de spare toujours en état de fonctionnement ;
- La traçabilité totale et en temps réel ;
- Une gestion des stocks de pièces détachées en interne.

Glossaire

Clients légers : Au sens matériel, un **client léger** est un ordinateur qui n'a presque pas de logique d'application (applications, logiciels). Il dépend donc surtout du serveur central sur lequel il se connecte et permet d'ouvrir des sessions utilisateurs.

CNIL : La **Commission nationale de l'informatique et des libertés** (**CNIL**) de France est une autorité administrative indépendante française. La CNIL est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Data Center : Un **centre de données** (en anglais *data center* ou *data centre*) est un lieu (et un service) regroupant des équipements constituants du système d'information d'une ou plusieurs entreprise(s) (ordinateurs centraux, serveurs, baies de stockage, équipements réseaux et de télécommunications, etc.). Il peut être interne et/ou externe à l'entreprise, exploité ou non avec le soutien de prestataires

Démarche ITIL : **ITIL** (**« Information Technology Infrastructure Library »** pour « Bibliothèque pour l'infrastructure des technologies de l'information ») est un ensemble d'ouvrages recensant les bonnes pratiques (« best practices ») du management du système d'information.

GLPI : **GLPI** (Gestionnaire Libre de Parc Informatique) est un logiciel libre de gestion des services informatiques (ITSM) et de gestion des services d'assistance (*issue tracking system* et *ServiceDesk*).

NAS : Un **serveur de stockage en réseau**, également appelé **stockage en réseau NAS**, **boîtier de stockage en réseau** ou plus simplement **NAS** (de l'anglais ***Network Attached Storage***), est un serveur de fichiers autonome, relié à un réseau dont la principale fonction est le stockage de données en un volume centralisé pour des clients réseau hétérogènes.

Pare-feu : Un **pare-feu** (de l'anglais *firewall*) est un logiciel et/ou un matériel permettant de faire respecter la politique de sécurité du réseau, celle-ci définissant quels sont les types de communications autorisés sur ce réseau informatique. Il surveille et contrôle les applications et les flux de données (paquets).

RGPD : Le **règlement nº 2016/679**, dit **règlement général sur la protection des données** (**RGPD**, ou encore **GDPR**, de l'anglais *General Data Protection Regulation*), est un règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il renforce et unifie la protection des données pour les individus au sein de l'Union européenne.

RPO : Recovery Point Objective : Durée des données qu'il est acceptable de perdre.

RTO : Recovery Time Objective : Temps nécessaire pour restaurer complètement le SI.

Sauvegarde différentielle : Avec la **sauvegarde différentielle**, seuls les fichiers modifiés depuis la dernière **sauvegarde** complète sont **sauvegardés**. C'est donc tout à fait normal si ce processus exige plus de temps mais aussi un plus grand espace de stockage par rapport à la **sauvegarde** incrémentale.

Sauvegarde incrémentielle : La **sauvegarde** incrémentielle ou incrémentale permet uniquement de **sauvegarder** les fichiers modifiés depuis dernière la **sauvegarde** précédente. Enfin, la **sauvegarde** différentielle copie toutes les données depuis le dernier backup incrémental ou complet.

Technologie SSD : En informatique un **SSD** (de l'anglais *solid-state drive*), appelé parfois **disque SSD,** est un matériel informatique permettant le stockage de données sur de la mémoire flash.

Sources : wikipédia

Webographie (sources)

Méthodologie

- http://www.eval.fr/methodes-et-outils/cadrelogique/analyse-des-problemes/
- http://www.ih2ef.education.fr/conseils/commande/operations/formuler-une-problematique/
- https://fr.slideshare.net/ardesimp/analyse-des-besoins
- https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
- https://www.cnil.fr/fr/principes-cles/rgpd-se-preparer-en-6-etapes

Sécurité

- http://www.spiralebackup.com/types-de-sauvegarde/
- https://www.economie.gouv.fr/files/170922_politiques-sauvegardes_v1.1.pdf
- https://www.informanews.net/perte-de-donnees-cause-faillite/
- https://www.scalair.fr/blog/strategie-sauvegarde-efficace
- https://www.ssi.gouv.fr/guide/mot-de-passe/
- https://www.cdse.fr/wifi-et-conservation-des-donnees
- https://www.quebeccloud.com/pourquoi-cest-important-de-definir-vos-rto-et-rpo/
- https://blog.advancia-itsystem.com/les-notions-de-rpo-et-rto-plan-reprise-dactivite/

Charte qualité :

- https://www.espace-technologie.com/wp-content/uploads/2015/10/et-charte-protection-donnees.pdf
- https://www.depanh24.fr/quality-convention/index.htm
- http://www.jcrinformatique.com/charte_qualite.php
- http://www.extensys-informatique.com/charte-qualite-informatique.php
- https://qualite.ooreka.fr/comprendre/charte-qualite

Charte informatique : Intranet CESI

Charte de confidentialité :

- https://www.legisocial.fr/actualites-sociales/2743-protection-donnees-personnelles-cadre-controle-outils-informatiques.html
- https://contrat-de-travail.ooreka.fr/ebibliotheque/voir/141172/clause-de-confidentialite

Mémo :

- https://www.iris-info.com/nos-solutions/externalisation-de-stock-de-spare/