kz

PROJET SAS 2019

Gestionnaire en maintenance et support informatique

Maxime SOURIS - Guillaume BURY – Amar GHAZANFAR
Bruce ANDRE-MATTA

CESi alternance
ÉCOLE SUPÉRIEURE DES MÉTIERS

Sommaire

I. Présentation de l'entreprise

Notre entreprise, « 4Bits Corporation », ayant pour principale activité la prestation informatique, souhaite obtenir la gestion du parc informatique (70 à 80 postes) du concessionnaire « AutoConcept ». Ce dernier souhaite externaliser les prestations informatiques aujourd'hui exécutées par deux informaticiens en internes. D'autres entreprises concurrentes sont aussi en courses.

Notre directeur technique nous charge de réaliser une partie de l'étude avant-vente et qu'en cas d'obtention du marché, l'un des deux informaticiens de l'entreprise « AutoConcept » sera recruté. Nous serons chargés de son accueil et son accompagnement au sein de notre entreprise.

SARL 4bits corporation établi à Reims (51100) au 128 avenue d'Epernay avec 14 employés pour 450k € de chiffres d'affaires en 2018 pour un capital de 170k €.

La société 4bits corporation se met à votre service en tant que spécialiste dans l'externalisation de vos services informatiques. Une expérience personnalisée vous sera proposée pour répondre à tous vos besoins en matière d'informatique, de logistique d'organisation et de sécurité informatique.

Vous bénéficierez de conseils et d'un suivi personnalisé, ainsi que nos techniciens qui seront à votre service en mettant nos outils à votre disposition.

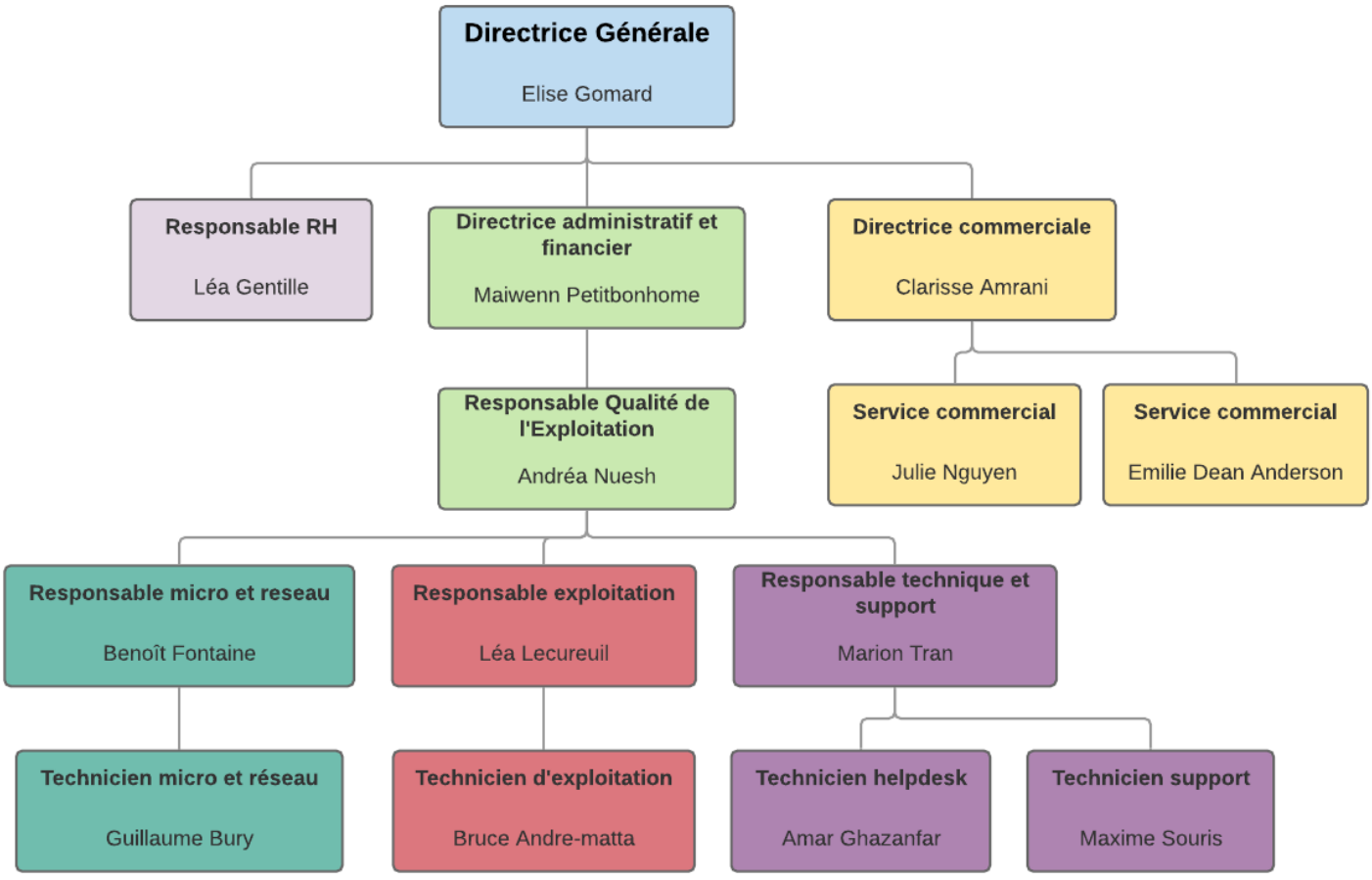
Nos principales activités sont :

- Maintenance préventive et curative de l'informatique
- Administration de parc
- Administration systèmes et réseaux
- Prospectives, équipements et achats informatiques
- Assistance logiciels, matériels, et utilisateurs à distance et sur site
- Gestion des comptes utilisateurs et sécurité informatique
- Formations utilisateurs

Nos coordonnées :

Adresse : 128 Avenue d'Epernay 51100 Reims
Téléphone : 03.82.65.58.63
Fax : 03.82.65.58.64
Mail : 4bits-ssii@4bits.fr

Organigramme de 4Bits corporation :

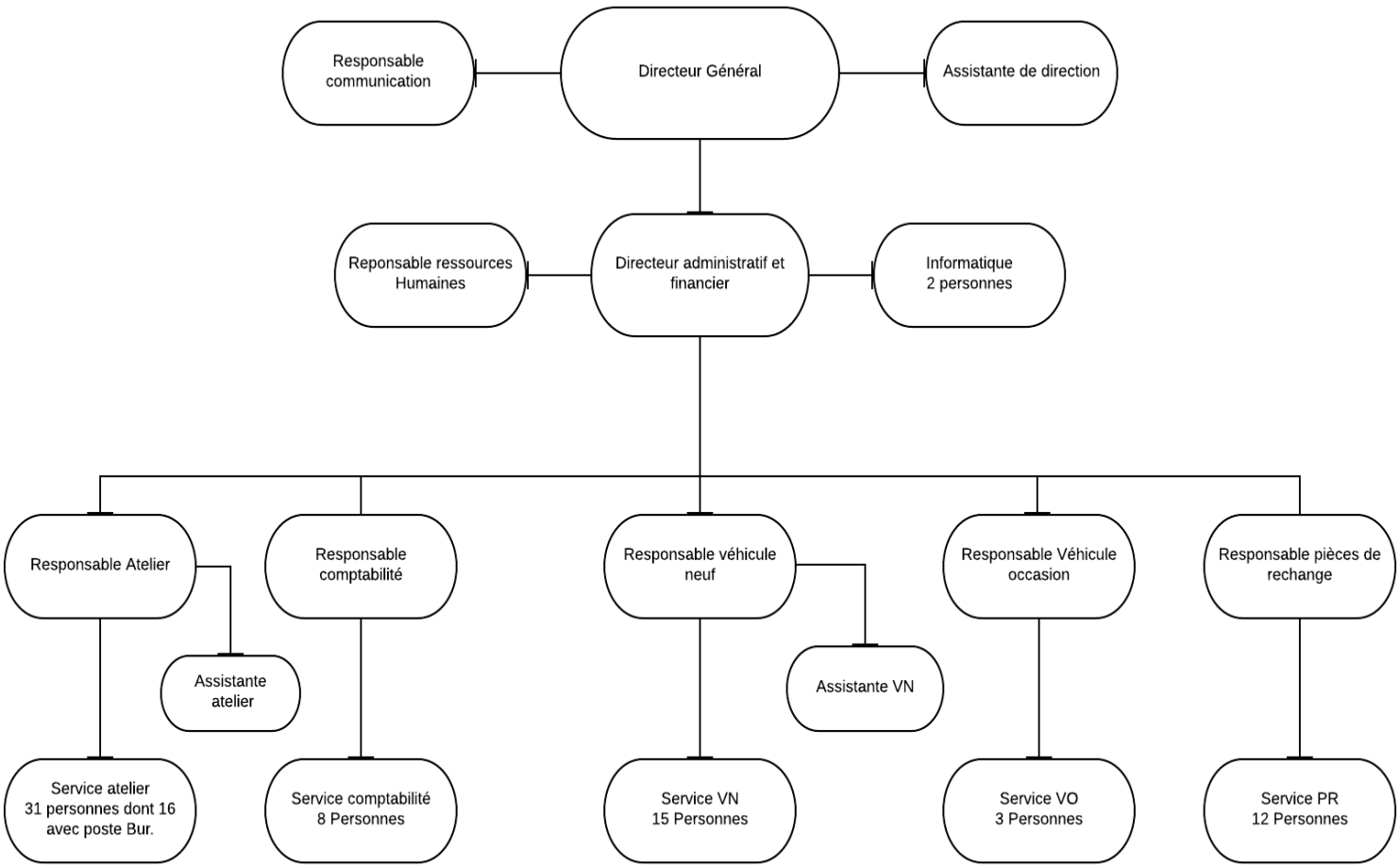


II. Présentation d'AutoConcept

AutoConcept est une concession automobile, qui souhaite externaliser ses prestations informatiques exécutées actuellement en interne par deux techniciens.

Activité : Commerce de voitures et de véhicules légers, neufs et d'occasions.

Organigramme d'AutoConcept



III. Synthèse des besoins du client

4bits apporte un soin particulier aux besoins de ses clients. C'est pour cela que 4Bits met en place la synthèse des besoins d'AutoConcept afin d'être prêt à y répondre de la manière la plus efficace et rapide possible.

I. Parc informatique

- Lenteurs de certains postes.
- Absence de sauvegardes.
- Manque d'informations clients.
- Absence et mauvaise gestion des mots de passes.

II. Posture des employés

- Confidentialité sur le site.
- Tenue vestimentaire des techniciens.
- Divulgation de données.
- Problème de langage.

III. Suivi technique

- Problème de délai d'intervention.
- Prise en charge et manque de suivis des incidents.

IV. Grille de risque AMDEC pour l'entreprise Auto-concept

Grille de risque présentant le taux de fréquence et de gravité de chaque incident. Un indice de criticité est additionné pour indiquer le taux d'importance des risques encourus. Une solution est proposée pour chaque cas.

Problématique	Niveau de probabilité	Gravité	Criticité	Solutions
Incendie	2	4	6	Sauvegardes externes
Foudre	1	4	5	Sauvegardes externes
Inondation	1	4	5	Sauvegardes externes
Séisme	1	4	5	Sauvegardes externes
Panne d'électricité	1	4	5	Groupe électrogène
Panne de switch	2	2	4	Switch de secours
Panne de poste informatique	1	1	3	Poste de rechange
Panne de serveur	2	4	6	Avoir un deuxième serveur en backup
Logiciels pas à jour	3	1	3	Activer mise à jour automatique / vérifier régulièrement les mise à jour à effectuer
Problème d'authentification du serveur lors des accès	2	2	4	Mise en place authentification serveur avant tout accès
Lenteur de postes	1	1	2	Ajout de SSD ou de ram supplémentaire sur postes lents/vieux
Problème de confidentialités	2	4	6	Ajout de mots de passes confidentiels et différents droits d'accès aux dossiers importants
Suivis des tickets	1	2	4	Répartition des tickets pour les différents techniciens
Non-respect des délais d'intervention	2	2	4	Respecter les heures prévues des interventions
Tenue des techniciens	1	1	2	Mise en place d'un mémo sur la tenue/comportement
Licences pirates	1	4	5	Normalisation du parc

V. Solutions proposées suite à la synthèse des besoins du client

À la suite des problématiques remontés à notre équipe technique, nous avons pu analyser et mettre au point des solutions en amont quant aux difficultés rencontrées par Autoconcept ;

1. Check up matériel et logiciel
    a. Inventorier les postes (Ajout de RAM et/ou SSD si besoin) voir remplacement du pc, avec une sauvegarde des données. Optimisation de la valorisation/obsolescence du matériel.
    b. Phase d'audit : serveurs, pc, switchs, logiciels, licences, imprimantes, scanners, câblages périphériques, site web, infrastructure réseau.
1. Mise en place de comptes nominatifs pour chaque utilisateur avec mots de passes confidentiels. Fiches récapitulatives + formations pour les mots de passes.
2. Sauvegarde complète hebdomadaire + sauvegarde incrémentielle quotidienne (plus fluide, plus rapide, plus adapté aux 80 postes) ainsi qu'une sauvegarde mensuelle sur site isolé.
    a. Un serveur de sauvegarde physique
    b. Un serveur de sauvegarde en cloud via entreprise tierce.
3. Création d'un support technique pour Autoconcept. Hotline 5J/7 de 8h à 18h et système de ticket 24h/7 avec prise en compte et catégorisation dans l'heure et suivis des tickets pour les utilisateurs. Ce système de ticket se fera à l'aide de notre logiciel "customer care" que nos équipes ont mis au point.
    a. Possibilité d'envois de techniciens sur place
    b. Prêt d'ordinateur si enlèvement du pc d'origine pour réparation à partir d'une journée.
4. Achats et investissements de matériel et de licences à la suite de l'audit. Proposition d'achat groupé à tarif préférentiel (bénéfice d'un certain %) même matériel pour plusieurs parc informatique, plus confortable pour les soucis de compatibilité de gestion et de maintenance entre les différentes entreprises.
5. Intégration de chartes de qualité, de confidentialité et charte informatique pour répondre aux besoins du client.
6. Propositions de solutions de stockage des données.
7. Prestation du fournisseur d'accès internet le mieux adapté à l'entreprise à externaliser.
8. Mémo interne sur le gage de qualité des techniciens de 4bits

VI. Nos engagements qualité

4bits-1 corporation a signé le 30 février 2019 une charte qui engage l'ensemble de nos collaborateurs à respecter 10 orientations fondamentales qui garantissent un service de qualité, transparent, qui promeut le meilleur usage des technologies et des systèmes d'information comme vecteur de création de valeur à nos clients.
L'objectif de cette Charte de Qualité est de fournir à nos clients potentiels une base d'échanges explicite qui décrit de manière précise les règles de conduite que les prestataires signataires s'engagent volontairement à respecter dans le cadre d'une relation commerciale de qualité.
4bits corporation est certifiée ISO 9001 : 2015 et fonde sa démarche Qualité sur deux grands principes :

- Satisfaire ses clients par le respect des engagements pris avec eux.
- Atteindre l'efficience par l'amélioration continue de ses processus pour obtenir le meilleur niveau d'efficacité à moindre coût.

L'engagement qualité de 4Bits est un facteur clé de différenciation pour ses clients et l'entreprise veille à ce que chacun soit impliqué dans les processus qualité afin de délivrer des services informatiques d'excellence. Cette charte et nos engagements

1. Clarté, Rigueur, Transparence : 4bits fourni des informations complètes et fiables tout au long de la prestation. 4bits s'efforce d'être clair dans ses explications en évitant notamment d'utiliser un jargon d'informaticien. 4bits souhaite rester compréhensible, n'hésitez pas à nous interroger si nous utilisons un terme que vous ne comprenez pas !

2. Accueil, Disponibilité, Réactivité : 4bits répond de manière rapide et adaptée à chaque demande. « 4bits customer care » est accessible 24/7 et notre hotline du lundi au samedi de 8h à 18h.

3. Personnalisation, Ecoute, Suivi : 4bits adapte sa prestation en fonction des attentes de ses clients. 4bits reste à l'écoute tout au long de sa prestation. 4bits assure le suivi de ses interventions et vérifie qu'il a véritablement répondu aux attentes de ses clients avant de clôturer un incident ou une demande.

4. Compétence, Expérience, Savoir-faire : 4Bits met au service des clients un intervenant compétent et professionnel ingénieur en informatique ou technicien. 4Bits possède 30 ans d'expérience de l'informatique pour les particuliers et les entreprises. 4Bits possède une expertise approfondie des problématiques, besoins et solutions informatiques. 4Bits est capable d'adapter son comportement et son mode opératoire à la diversité des situations rencontrées et des attentes de ses clients.

5. Confidentialité, Respect, Discrétion : 4Bits respecte la vie privée et l'intimité de ses clients. 4Bits préconise l'intervention à domicile, cela permet de garantir la confidentialité et la non-divulgation de vos données privées, car elles ne sortiront pas de chez vous !

6. Qualité, Evaluation, Amélioration : 4Bits fait évoluer ses pratiques pour améliorer la satisfaction de ses clients. 4Bits effectue un suivi de la satisfaction de ses clients notamment sous forme de questionnaire.

7. Durabilité, Robustesse, Fiabilité : 4Bits résout les problèmes de manière durable et vous explique comment les éviter à l'avenir. Son client n'a pas à craindre que le même problème réapparaisse au bout de quelques jours après l'intervention parce qu'il n'aura pas été correctement résolu.

8. Objectivité, Ouverture, Neutralité : 4Bits agit en toute neutralité par rapport aux solutions du marché. 4Bits n'a contracté avec aucun fabricant, éditeur ou prestataire. 4Bits est ouvert à toutes les solutions marché afin de pouvoir conseiller la meilleure à son client.

9. Optimisation : Dans un souci d'optimisation des dépenses de ses clients, 4Bits préfère que ses clients achètent en direct chez les fournisseurs, au meilleur prix. 4Bits se positionne en tant que conseiller. Cela permet par exemple, en fonction du contexte de se laisser le choix entre le neuf et l'occasion. Néanmoins, à la demande de son client (et pour assurer un service complet), 4Bits peut revendre des matériels, logiciels ou services tiers.

10. Economie : Dans un souci d'économie pour son client, 4Bits effectue le strict nécessaire pour répondre aux besoins exprimés, ni plus ni moins ! Toute amélioration complémentaire, mais non indispensable, ne sera effectuée qu'avec l'accord du client, en toute transparence. 4Bits se positionne en tant que conseil, mais c'est au client qu'appartient la décision finale.

Nouveau. RGPD : Depuis le 25 Mai 2018, le règlement européen pour la protection des données personnelles est entré en vigueur. Modifiant l'approche de la protection des données personnelles, 4Bits corporation affirme sa conformité à la RGPD. Aussi, dans un souci de clarté 4Bits propose une série de conseils et de suivi des règlements mis en place par la RGPD.

VII. La protection des données

4Bits corporation vous propose également un plan de sécurisation et de protection de vos données :

I. Mesures immédiates de sauvegarde

- Mise en place d'un système de backup en réplication sur 3 sites.
- Sauvegarde totale des données d'Autoconcept à la suite de la signature du contrat et de la 1ère intervention des techniciens de 4Bits corporation.
- Mise en place d'un système de sauvegarde hebdomadaire, quotidienne, et mensuelle en réplication sur site et dans les data center de backup en raid 51.

II. Protéger les accès aux services

Il est important de règlementer l'accès aux différents niveaux des structures d'une entreprise notamment pour éviter tout menace externe ou interne à l'entreprise, pour cela la mise en place des mesures de sécurité comme d'un système d'accès par badges, dispositifs divers de surveillance et alarmes sont recommandés. Il est aussi recommandé à l'employer de veiller et signaler tout personne non autorisée circulant dans les locaux.

III. La gestion des accès informatiques

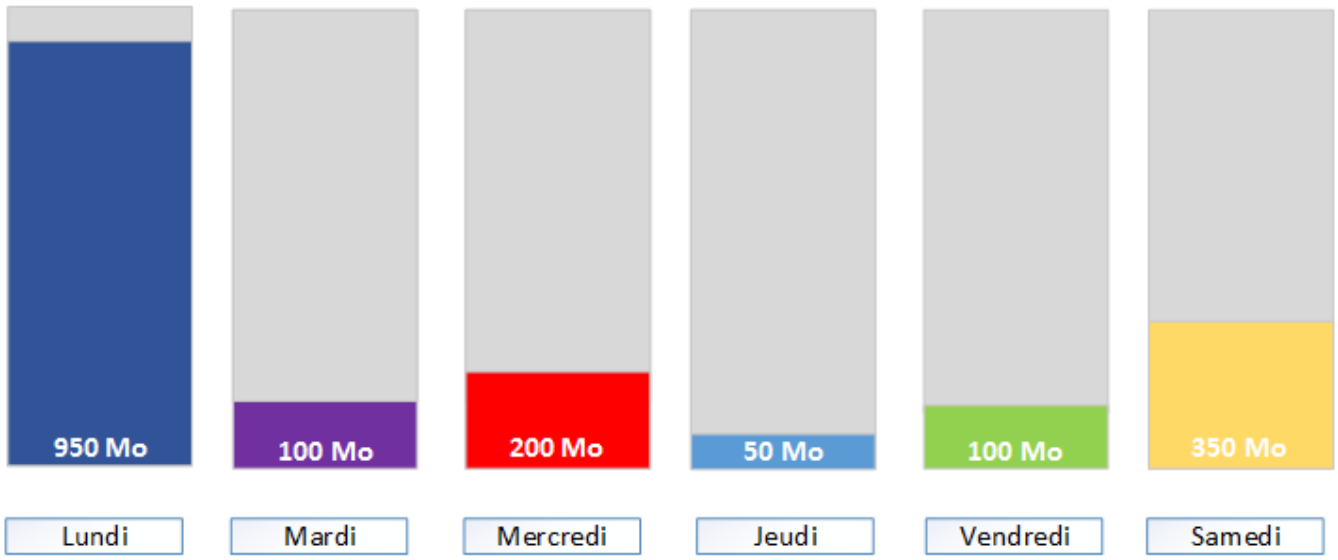
Dans un premier temps il est important de renforcer la sécurité du système informatique de l'entreprise notamment avec l'aide d'une politique de mot de passe. Ce mot de passe devra respecter certaine règle de complexité notamment :

- 8 caractères minimum de types 3 différents (majuscules, minuscules, chiffres, caractères spéciaux).
- Il devra être renouvelé tous les 90 jours.
- Ne pas stockez les mots de passe dans un fichier sur un poste informatique ou sur papier.
- Il ne doit pas être lié à l'identité de l'utilisateur.

Il convient aussi de mettre en place des hiérarchies de profils, avec différents niveaux d'habilitation, pour que les accès aux données soient restreints de sorte que chaque salariés ou intervenant externe n'aient accès qu'aux applications et aux données dont ils ont besoin dans le cadre de leurs fonctions.

IV. Les systèmes de sauvegarde

Pour la mise en place de notre système de sauvegarde nous avons opté pour la méthode incrémentale, ce processus de sauvegarde permet de sauvegarder le sous-ensemble d'un composant qui fait l'objet d'une modification depuis la dernière session, ensuite ce procédé marque l'ensemble des fichiers afin de différencier les données déjà sauvegarder et celle non sauvegarder. Ainsi plus performante et plus rapide qu'une sauvegarde complète, la sauvegarde incrémentielle permet de cibler les fichiers modifier et profiter d'un espace de stockage plus faible.

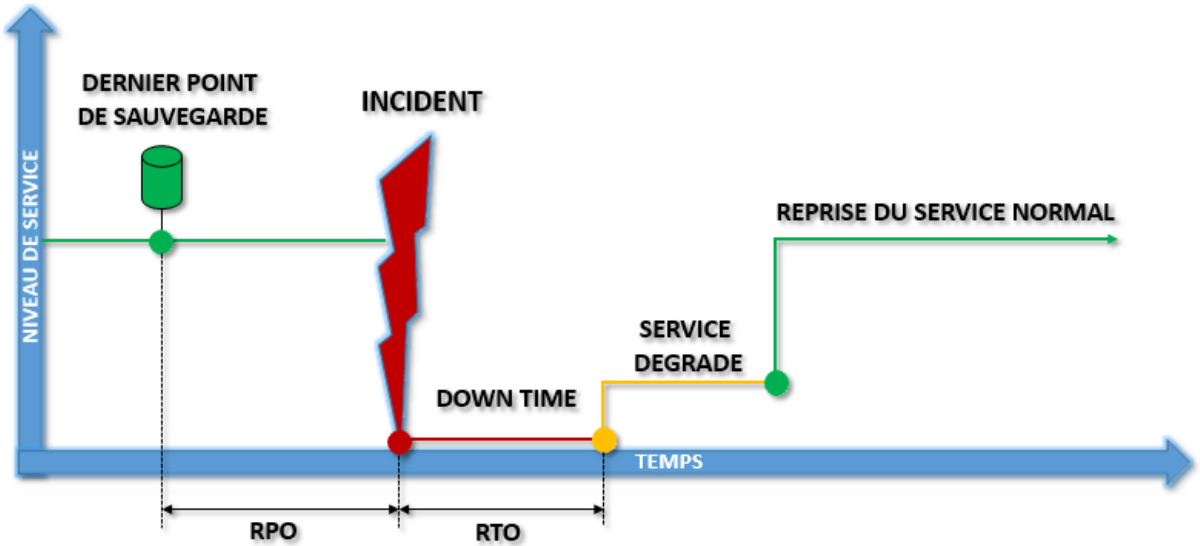


https://www.it-connect.fr/wp-content-itc/uploads/2015/03/sauvegar-incrementielle-01.png

Sauvegarde incrémentielle :

Système permettant de sauvegarder uniquement les données modifiées ou ajoutées depuis la dernière sauvegarde.

Le risque zéro n'existant pas, il est important de mettre en place en cas de panne, une « *durée maximale d'interruption admissible* »(RTO), cette durée est fixée en fonction des besoins de production vis-à-vis de la ressource informatique. La durée « *maximale d'enregistrement des données qu'il est acceptable de perdre lors d'une panne* » (RPO) doit être suffisamment courte pour ne pas engendrer de perte critique, ce qui permet la continuité de l'activité.



https://i2.wp.com/blog.advancia-itsystem.com/wp-content/uploads/2018/09/RTO-RPO2.png?resize=787%2C361&ssl=1

Pour cela nous avons fait un planning de sauvegarde des données.

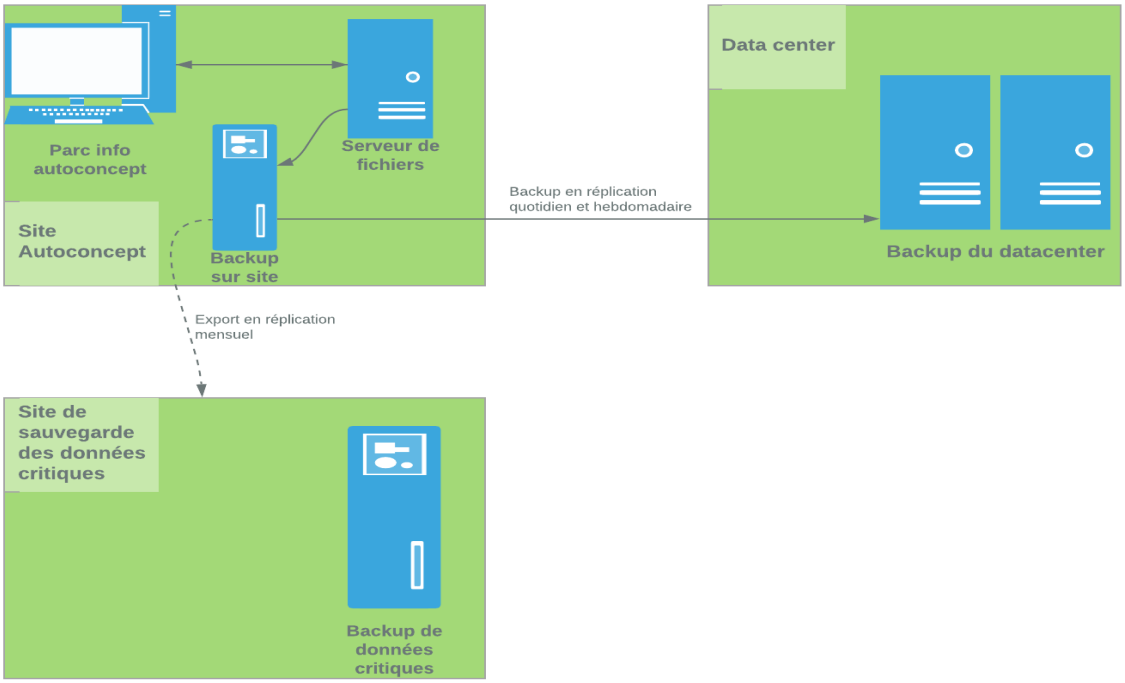
Lundi	**Mardi**	**Mercredi**	**Jeudi**	**Vendredi**	**Samedi**	**Dimanche**
Sauvegarde incrémentielle A minuit	Sauvegarde incrémentielle A minuit	Sauvegarde incrémentielle A minuit	Sauvegarde incrémentielle A minuit	Sauvegarde incrémentielle A minuit	Sauvegarde incrémentielle A minuit	Sauvegarde complète

- Sauvegarde quotidienne des données.
- Conservation des sauvegardes quotidiennes durant une semaine. Restauration possible des données à J-1, J-2, J-3, J-4, J-5, J-6, J-7.
- Au-delà des 7 premiers jours, conservation d'une sauvegarde par semaine pendant un mois. Restauration possible des données à J-14, J-21, J-28
- Au-delà du premier mois, conservation d'une sauvegarde par mois pendant un an. Restauration possible des données à M-1, M-2, M-3, M-4, M-5, M-6, M-7, M-8, M-9, M-10, M-11, M-12.
- Accès à 22 sauvegardes au bout d'un an.

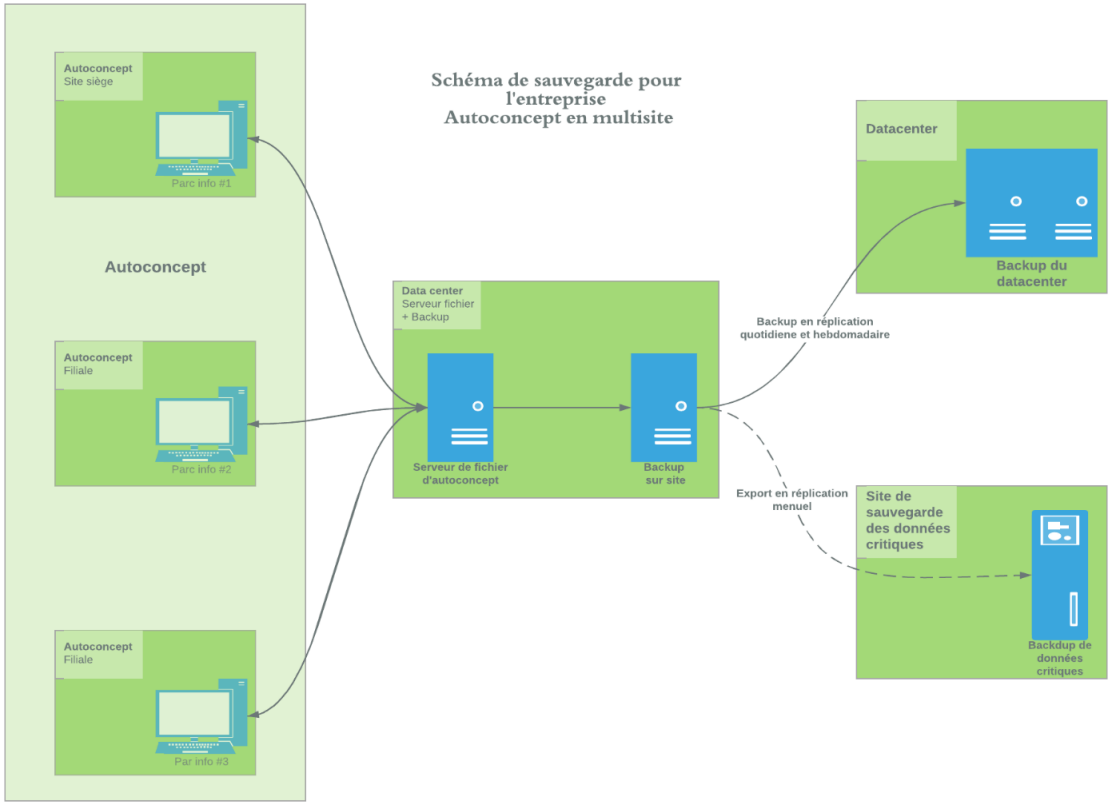
" https://www.open-dsi.fr/strategie-retention-sauvegardes/ "

Voici les propositions d'externalisation des ressources informatique de 4Bits Corporation proposé à AutoConcept.

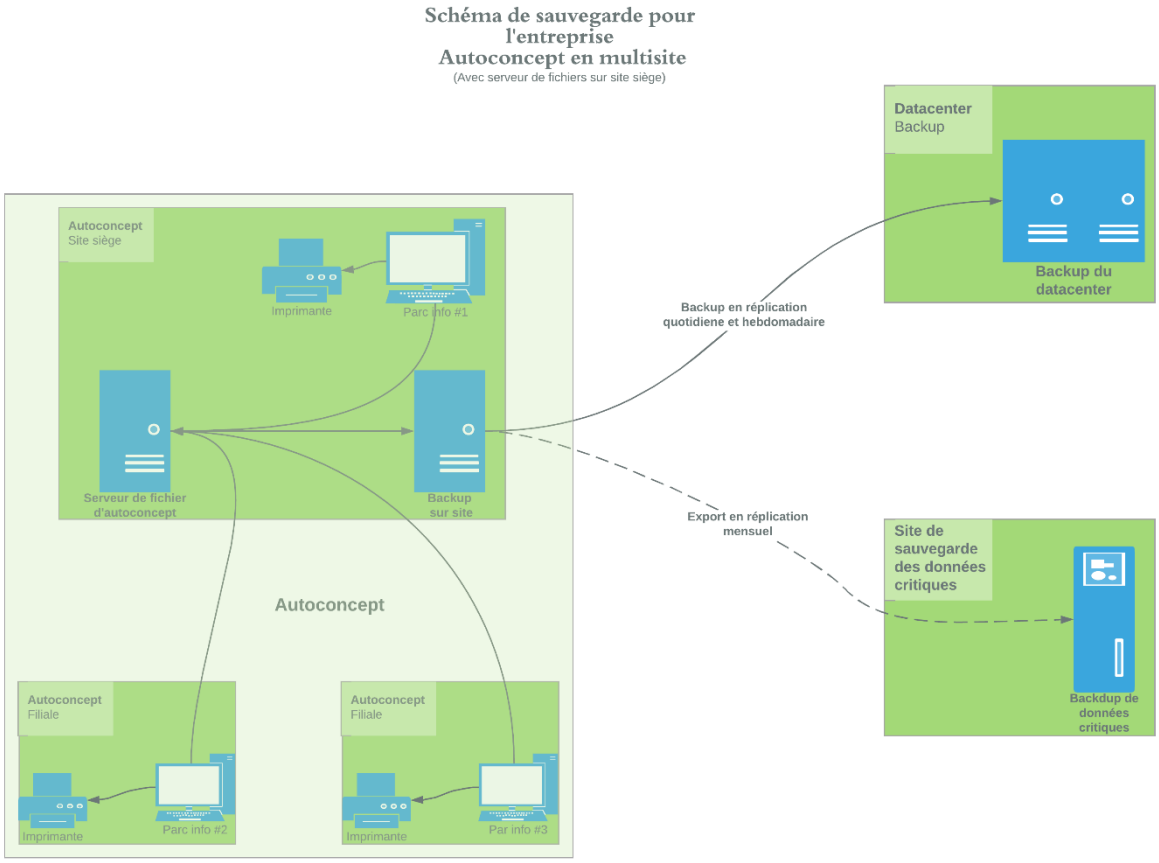
En cas de sauvegarde des données sur un site



En cas d'une sauvegarde multisite



En cas d'une sauvegarde multisite avec Serveur de fichier sur site siège



VIII. Note de changement de sécurisation des données

Note distribuée à l'ensemble de nos clients.

Mesdames, Messieurs,

L'entreprise 4Bits vous informe d'un changement de sécurisation de vos données.
Ce changement concerne vos mots de passe. Nous vous rappelons que ceux-ci sont STRICTEMENT PERSONNEL ET CONFIDENTIEL. En aucun cas et sous aucun prétexte ils ne devront être divulgués à un tier.
Le nouveau mot de passe doit comporter :

- 8 caractères minimum de 3 types différents (majuscules, minuscules, chiffres, caractères spéciaux).
- Il devra être renouvelé tous les 90 jours.
- Ne pas stockez les mots de passe dans un fichier sur un poste informatique ou sur papier.
- Il ne doit pas être lié à l'identité de l'utilisateur.

La société 4bits vous invite à prendre en compte ce changement et à adopter une attitude responsable :
Verrouillez votre session dès que vous quittez votre poste de travail.
En outre, il ne doit contenir aucune info personnelle et devra être réinitialisé au maximum tous les 90 jours. Un rappel vous sera envoyé dans votre boite mail.

4Bits mettra également en place une hiérarchisation des profils, avec différents niveaux d'habilitations pour que les accès aux données soient restreints.

Ce changement prendra effet lors de votre prochaine ouverture de session. Un programme clair et ludique vous guidera pas à pas.

Merci de votre compréhension,
L'équipe de 4bits reste à votre entière disposition en cas de nécessité.

Cordialement,

L'équipe 4bits.

IX. Charte informatique

4Bits corporation vous propose une charte informatique applicable à Autoconcept.

1. Préambule

4Bits corporation propose à ses clients et ses collaborateurs une charte informatique à valeur juridique. Celle-ci définit les conditions générales d'utilisation des systèmes d'informations et de communications au sein de 4bits et des entreprises clientes.
Cette charte sera distribuée à chaque employés, elle devra être lue et signée par les différents utilisateurs présent sur le réseau. En outre elle informe les personnes visées des outils mis à disposition et des différents usages possible. En outre cette charte vise à établir des sanctions en cas de manquement aux règlements et à la loi en vigueur.

2. Champ d'application

2.1/ L'Utilisateurs concernés

Sauf mention contraire, la présente charte s'applique à l'ensemble des utilisateurs du système d'information et de communication de l'entreprise, quel que soit leur statut, y compris les mandataires sociaux, salariés, intérimaires, stagiaires, employés de sociétés prestataires, visiteurs occasionnels.

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

2.2/ Système d'information et de communication

Le système d'information et de communication de l'entreprise est notamment constitué des éléments suivants : ordinateurs (fixes ou portables), périphériques, assistants personnels, réseau informatique (serveurs, routeurs et connectique), photocopieurs, téléphones, logiciels, fichiers, données et bases de données, système de messagerie, intranet, extranet, abonnements à des services interactifs.

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

3. Confidentialité

3.1/ Paramètre d'accès

L'utilisation et l'accès au système d'information de l'entreprise (comme la messagerie électronique ou téléphonique, les sessions sur les postes de travail, le réseau, certaines applications ou services interactifs) est protégé par des paramètres d'identification et d'authentification (identifiant, mot de passe). Il ne doit pas utiliser de comptes autres que ceux auxquels il a légitimement accès, il ne doit pas masquer son identité de quelque façon que ce soit.

Ces mesures de sécurité permettent de contrôler l'activité des employés. Les paramètre d'accès, dans la mesure du possible doivent être mémorisés par l'utilisateur et ne pas être conservés, sous quelque forme que ce soit, ils sont strictement confidentiels et ne doivent être communiqué à personne.

Lorsqu'ils sont choisis par l'utilisateur, les paramètres doivent respecter un certain degré de complexité (8 caractères minimum de types 3 différents (majuscules, minuscules, chiffres, caractères spéciaux) et être modifiés régulièrement (Il devra être renouvelé tous les 90 jours). Des consignes de sécurité sont élaborées par 4bits corporation afin de recommander les bonnes pratiques en la matière en accord avec notre politique de mots de passe.

3.2/ Données

L'utilisateur est responsable des informations qu'il est amené à consulter ou détenir dans l'exercice de ses fonctions. Il ne doit ni lire, ni copier les fichiers d'un autre utilisateur qui ne sont pas dans l'espace public, sans son autorisation verbale ou écrite. Les fichiers mis en réseau sont en lecture seule et ne peuvent pas être modifiés, sauf accès spécifique directionnel. Il doit être vigilant sur le risque de divulgation dans l'utilisation des outils personnel ou appartenant à l'entreprise en dehors des locaux de l'entreprise.

4. Sécurité

4.1/ Rôle de l'entreprise

L'entreprise met à disposition des moyen humain et technique pour prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès.

L'entreprise est responsable du contrôle du bon fonctionnement du système d'information et de communication. Elle veille à l'application des règles de la présente charte Les membres du service informatique sont assujettis à une obligation de confidentialité sur les informations qu'ils sont amenés à connaître.

4.2/ Responsabilité de l'utilisateur

L'utilisateur est responsable quant à lui des ressources qui lui sont confiées dans le cadre de l'exercice de ses fonctions. Il doit concourir à la protection des dites ressources, en faisant preuve de prudence. Il doit également veiller à se déconnecter de sa session à chaque fois qu'il quitte son poste de travail.

En cas d'absence, même temporaire, il est impératif que l'utilisateur verrouille l'accès au matériel qui lui est confié ou à son propre matériel, dès lors que celui-ci contient des informations à caractère professionnel.

Pour des raisons de sécurités les utilisateurs ne devront pas amener leur propre matériel informatique dans l'entreprise qu'il s'agisse d'un ordinateur, d'une tablette ou d'un téléphone. Si besoin du matériel adapté seras prêté à l'employé avec obligatoirement une feuille de mise à disposition daté et signée par la personne concernée.

En cas d'accès au système d'information avec du matériel n'appartenant pas à l'entreprise (assistants personnels, supports amovibles…), il appartient à l'utilisateur de veiller à la sécurité du matériel utilisé et à son innocuité.

L'utilisateur doit effectuer des sauvegardes régulières des fichiers dont il dispose sur le matériel mis à sa disposition et selon les procédures fournies par le service informatique. Il doit également supprimer de manière régulière des données devenues inutiles sur les espaces communs du réseau. Les données anciennes qu'ils souhaite conserver doivent être archivées en accord avec la direction informatique et des procédures prévues à cet effet.

L'utilisateur doit éviter d'installer des logiciels, de copier ou d'installer des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. Il doit dans tous les cas en alerter le service informatique.

L'utilisateur veille au respect de la confidentialité des informations en sa possession. Il doit en toutes circonstances veiller au respect de la législation, qui protège notamment les droits de propriété intellectuelle, le secret des correspondances, les données personnelles, les systèmes de traitement automatisé de données, le droit à l'image des personnes, l'exposition des mineurs aux contenus préjudiciables. Il ne doit en aucun cas se livrer à une activité concurrente à celle de l'entreprise ou susceptible de lui causer un quelconque préjudice en utilisant le système d'information et de communication

5. Internet

5.1/ Accès aux sites

Dans le cadre de leur activité, les utilisateurs peuvent avoir accès à Internet. Pour des raisons de sécurité, l'accès à certains sites peut être limité ou prohibé par le service informatique. Celui-ci est habilité à imposer des configurations du navigateur et à restreindre le téléchargement de certains fichiers.

5.2/ Autres utilisations

La contribution des utilisateurs à des forums de discussion, systèmes de discussion instantanée, blogs, sites est autorisée, sous réserve de permission préalable du service informatique. Un tel mode d'expression est susceptible d'engager la responsabilité de l'entreprise, une vigilance renforcée des utilisateurs est donc indispensable.

Il est rappelé que les utilisateurs ne doivent en aucun cas se livrer à une activité illicite ou portant atteinte aux intérêts de l'entreprise, y compris sur Internet.

6. Messagerie électronique

La messagerie électronique est un moyen d'amélioration de la communication au sein des entreprises et avec les tiers. Chaque salarié dispose, pour l'exercice de son activité professionnelle, d'une adresse de messagerie électronique attribuée par le service informatique.

Les messages électroniques reçus sur la messagerie professionnelle font l'objet d'un contrôle antiviral et d'un filtrage anti-spam. Les salariés sont invités à informer le service informatique des dysfonctionnements qu'ils constatent dans le dispositif de filtrage.

6.1/ Conseils généraux

L'attention des utilisateurs est attirée sur le fait qu'un message électronique a la même portée qu'un courrier manuscrit et peut rapidement être communiqué à des tiers. Il convient de prendre garde au respect d'un certain nombre de principes, afin d'éviter les dysfonctionnements du système d'information, de limiter l'envoi de messages non sollicités et de ne pas engager la responsabilité civile ou pénale de l'entreprise et/ou de l'utilisateur.

L'envoi de messages électroniques à des tiers obéit aux mêmes règles que l'envoi de correspondances postales, en particulier en termes d'organisation hiérarchique. En cas de doute sur l'expéditeur compétent pour envoyer le message, il convient d'en référer à l'autorité hiérarchique.
Avant tout envoi, il est impératif de vérifier l'identité des destinataires du message et de leur qualité à recevoir communication des informations transmises.

En cas d'envoi à une pluralité de destinataires, l'utilisateur doit respecter les dispositions relatives à la lutte contre l'envoi en masse de courriers non sollicités. Il doit également envisager l'opportunité de dissimuler certains destinataires, en les mettant en copie cachée, pour ne pas communiquer leur adresse électronique à l'ensemble des destinataires. En cas d'envoi à une liste de diffusion, il est important de vérifier la liste des abonnés à celle-ci, l'existence d'archives accessibles par le public et les modalités d'abonnement.

La vigilance des utilisateurs doit redoubler en présence d'informations à caractère confidentiel. Les messages doivent dans ce cas être cryptés, conformément aux recommandations du service informatique.

Le risque de retard, de non remise et de suppression automatique des messages électroniques doit être pris en considération pour l'envoi de correspondances importantes. Les messages importants sont envoyés avec un accusé de réception OU signés électroniquement. Ils doivent, le cas échéant, être doublés par des envois postaux.

Les utilisateurs doivent veiller au respect des lois et règlements, et notamment à la protection des droits de propriété intellectuelle et des droits des tiers. Les correspondances électroniques ne doivent comporter aucun élément illicite, tel que des propos diffamatoires, injurieux, contrefaisants ou susceptibles de constituer des actes de concurrence déloyale ou parasitaire.

La forme des messages professionnels doit respecter les règles définies par le service informatique, notamment en ce qui concerne la mise en forme et la signature des messages.

Le service informatique de l'entreprise doit être informé de toute absence supérieure à 3 jour(s), afin de mettre en place un répondeur automatique.

6.2/ Limites techniques

La taille, le nombre et le type des pièces jointes peuvent être limités par le service informatique pour éviter l'engorgement du système de messagerie.

Les messages électroniques sont conservés pendant une durée de 1ans. Passé ce délai, ils sont automatiquement archivés OU supprimés. Si le salarié souhaite conserver des messages au-delà de ce délai, il lui appartient d'en prendre copie.

6.3/ Utilisation personnelle de la messagerie

Les messages à caractère personnel sont tolérés, à condition de respecter la législation en vigueur, de ne pas perturber et de respecter les principes posés dans la présente charte.

Les messages envoyés doivent être signalés par la mention " Privé " dans leur objet et être classés dès l'envoi dans un dossier lui-même dénommé " Privé ". Les messages reçus doivent être également classés, dès réception, dans un dossier lui-même dénommé " Privé ". En cas de manquement à ces règles, les messages sont présumés être à caractère professionnel.

Les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de message à caractère personnel.

Afin d'éviter l'interception de tout message destiné à une institution représentative du personnel, les messages présentant une telle nature doivent être signalés et classés de la même manière que les messages à caractère personnel.

7. Données personnelles

La loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, définit les conditions dans lesquelles des traitements de données personnels peuvent être opérés. Elle institue au profit des personnes concernées par les traitements des droits que la présente invite à respecter, tant à l'égard des utilisateurs que des tiers.

Des traitements de données automatisés et manuels sont effectués dans le cadre des systèmes de contrôle, prévus dans la présente charte. Ils sont, en tant que de besoin, déclarés conformément à la loi du 6 janvier 1978.

Il est rappelé aux utilisateurs que les traitements de données à caractère personnel doivent être déclarés à la Commission nationale de l'informatique et des libertés, en vertu de la loi n° 7817 du 6 janvier 1978. Les utilisateurs souhaitant réaliser des traitements relevant de ladite loi sont invités à prendre contact avec le service informatique de l'entreprise avant d'y procéder.

8. Contrôles des activités

8.1/ Contrôles automatisés

Le système d'information et de communication s'appuie sur des fichiers journaux " logs ", créés en grande partie automatiquement par les équipements informatiques et de télécommunication. Ces fichiers sont stockés sur les postes informatiques et sur le réseau. Ils permettent d'assurer le bon fonctionnement du système, en protégeant la sécurité des informations de l'entreprise, en détectant des erreurs matérielles ou logicielles et en contrôlant les accès et l'activité des utilisateurs et des tiers accédant au système d'information.

Les utilisateurs sont informés que de multiples traitements sont réalisés afin de surveiller l'activité du système d'information et de communication. Sont notamment surveillées et conservées les données relatives :

- à l'utilisation des logiciels applicatifs, pour contrôler l'accès, les modifications suppression de fichiers ;

- aux connexions entrantes et sortantes au réseau interne, à la messagerie et à Internet, pour détecter les anomalies liées à l'utilisation de la messagerie et surveiller les tentatives d'intrusion et les activités, telles que la consultation de sites web ou le téléchargement de fichiers.

L'attention des utilisateurs est attirée sur le fait qu'il est ainsi possible de contrôler leur activité et leurs échanges. Des contrôles automatiques et généralisés sont susceptibles d'être effectués pour limiter les dysfonctionnements, dans le respect des règles en vigueur.

8.2/ Procédure de contrôle manuel

En cas de dysfonctionnement constaté par le service informatique, il peut être procédé à un contrôle manuel et à une vérification de toute opération effectuée par un ou plusieurs utilisateurs.

Lorsque le contrôle porte sur les fichiers d'un utilisateur et sauf risque ou événement particulier, le service informatique ne peut ouvrir les fichiers identifiés par le salarié comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. Le contenu des messages à caractère personnel des utilisateurs (tels que définis à l'article 4 des présentes), ne peut en aucun cas être contrôlé par le service informatique.

9. Information et sanctions

9.1/ Sanction

Le manquement aux règles et mesures de sécurité de la présente charte est susceptible d'engager la responsabilité de l'utilisateur et d'entraîner à son encontre des avertissements, des limitations ou suspensions d'utiliser tout ou partie du système d'information et de communication, voire des sanctions disciplinaires, proportionnées la gravité des faits concernés conformément au règlement intérieur de chaque entreprise et de la loi en vigueur.

Dès lors qu'une sanction disciplinaire est susceptible d'être prononcée à l'encontre d'un salarié, celui-ci est informé dans un bref délai des faits qui lui sont reprochés, sauf risque ou événement particulier

L'employeur peut être tenu pour responsable de l'utilisation des moyens qu'il met à disposition de ses salariés. Il est de son devoir d'utiliser son pouvoir et d'encadrer ces moyens par les dispositions qui lui sont accordées.

De ce fait un registre des activités de traitement peut être tenu, toute violation de données à caractère personnel peut faire l'objet d'une notification à la Commission nationale de l'informatique et des libertés et communique à la personne concernée.

9.1/ Information

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

Le service informatique est à la disposition des salariés pour leur fournir toute information concernant l'utilisation des NTIC (Ensemble des techniques utilisées pour le traitement et la transmission des informations (câble, téléphone, Internet, etc.)). Il informe les utilisateurs régulièrement sur l'évolution des limites techniques du système d'information et sur les menaces susceptibles de peser sur sa sécurité.

La présente charte et l'ensemble des règles techniques sont disponibles sur l'intranet de l'entreprise.

Des opérations de communication internes seront organisées, de manière régulière, afin d'informer les salariés sur les pratiques d'utilisation des NTIC recommandées.

10. Entrée en vigueur

La présente charte est applicable à compter du ……

Elle a été adoptée après information et consultation OU du comité d'entreprise OU des délégués du personnel en date du……

X. Politique de confidentialité

1. Domaine d'application

Afin de contribuer à l'externalisation du système informatique de nos clients, 4Bits Corporation décide d'établir sa politique de confidentialité à destination des acteurs qui interviennent sur site ou à distance pour nos différents clients.

Elle a pour but de préciser les responsabilités de 4Bits Corporation en accord avec la législation afin de garantir un usage correct des ressources informatiques et des services internet.

2. Obligation

4Bits Corporation est tenue à une obligation de discrétion sur les prestations qu'elle fournit à ses clients. En conséquence, 4Bits Corporation s'engage à ne pas évoquer ce sur quoi ils travaillent ou autres informations confidentielles, sauf dérogation fournie par les clients.

3. Objet

Sont confidentielles les informations dont la diffusion et l'exploitation à l'extérieur comme à l'intérieur est restreinte.

- Toutes les données relatives que l'on retrouve dans les scénarios de criticité de l'audit sécurité.
- Toutes les données relatives à l'architecture des SI
- Toutes les données personnelles relevant de la Commission Nationale de l'Informatique et des Libertés (CNIL)

4. Informations confidentielles

Les règles applicables aux informations confidentielles sont toutes applicables aux informations sensibles. Seuls peuvent avoir accès aux informations sensibles, les salariés de 4Bits Corporation qui y sont nominativement autorisés par les clients.

L'autorisation donnée à un salarié de 4Bits Corporation ne vaudra que pour un dossier ou une affaire précise. La direction ou la hiérarchie du salarié de 4Bits Corporation précisera, par écrit au client, quels sont les autres salariés autorisés à accéder aux données sur le dossier comportant des informations sensibles.

5. Divulgation des informations

4Bits Corporation s'interdit d'évoquer les informations confidentielles. Le salarié de 4Bits Corporation qui serait autorisé à traiter des informations sensibles dans un dossier précis, s'engage à ne pas évoquer ce dossier au sein de son entreprise, sauf aux personnes autorisées dont le nom lui aura été communiqué par la direction.

Cette obligation de confidentialité s'exerce aussi à l'égard du personnel des clients et de tout tiers en général.

De manière générale, 4Bits Corporation s'engage à respecter la présente charte de confidentialité aussi longtemps que lesdites informations n'auront pas été portées à la connaissance de tiers par le client lui-même.

6. Sortie de document ou matériel

4Bits Corporation s'interdit d'emporter, sauf nécessité de service, des documents hors des locaux de ses clients. S'il s'agit de documents comportant des informations confidentielles, il devra préalablement avoir obtenu une autorisation du client.

4Bits Corporation s'interdit d'envoyer des données confidentielles par Internet. En cas de nécessité absolue, et admise par la DSI, il lui demandera de manière prioritaire de remplacer toutes les données confidentielles par des données de type « test ». A défaut, les fichiers devront être envoyés par un canal sécurisé ou être cryptés. Les informations transmises sont couvertes par le secret des correspondances.

Si un employé de 4bits Corporation doit reprendre du matériel appartenant à ses clients, pour pratiquer un échange standard, dans le cadre d'une maintenance, 4Bits Corporation s'engage à effacer toutes les données d'un périphérique, avant de renvoyer ce matériel au constructeur ou à un quelconque fournisseur. De manière prioritaire, il devra laisser le temps à la DSI de pratiquer elle-même l'effacement des données. 4Bits Corporation s'engage à ne faire aucune extraction de données sans l'autorisation expresse du client.

7. Discrétion

4bits s'interdit de rechercher dans les documents, base de données ou fichier de ses clients quelconque information dont il n'aurait pas strictement besoin pour remplir sa mission.

8. Conservation d'information

4bits s'engage à n'enregistrer les informations sensibles que sur des supports sécurisés et à ne pas les divulguer à d'autres partenaires.

9. Suppression d'information

4 Bits s'engage à ne pas jeter les documents contenant des informations confidentielles ainsi que tout support logique ou physique.

10. CIL

Le correspondant informatique et liberté a été créé par la réforme de 2004 de la Loi Informatique et Liberté et par son décret d'application de 2005. Le CIL se positionne

en intermédiaire entre le responsable des traitements des données concernées (l'entreprise dans un contexte marketing) et la CNIL.

Le CIL est responsable :

- De la création et de la mise à jour d 'une liste des traitements effectués
- De la publicité de cette liste
- D'une fonction conseil et de recommandation auprès des responsables des traitements
- De l'intermédiation CNIL / structure
- D'une fonction d'alerte

A ce titre toute modification ou mise en service de matériels ou de programmes, comportant des données confidentielles et devant faire l'objet d'une déclaration auprès de la CNIL, devra être immédiatement signalé au correspondant CNIL, afin qu'il puisse faire les démarches nécessaires. https://www.data.gouv.fr/fr/datasets/correspondants-informatique-et-libertes-cil/ https://www.cnil.fr/fr/definition/correspondant-informatique-et-libertes

11. Télémaintenance

Dans le cadre d'une télémaintenance, tous les articles de cette présente charte sont applicables. Nos clients devront accepter que la prise en main à distance puisse être supervisée par un technicien de 4Bits Corporation.

12. Obligation

4Bits s'engage à informer ses clients, sous 48 heures de toutes anomalies, fuite d'informations ou risques dont il pourrait avoir connaissance.

13. Engagement

4Bits s'engage à se soumettre à tout audit ou contrôle demandé par ses Clients.

14. Respect de la Charte

Le non-respect de cette charte par 4Bits peut entrainer une rupture de tous les contrats avec nos clients et pourra être poursuivi en justice.

XI. Conclusion du projet SAS

Grâce à ce projet nous avons pu confronter nos idées et nos caractères afin de répondre à cet exercice d'appel d'offre.

Nous avons pu réaliser ce que représentait le fait de travailler en équipe, notamment sur la coopération et le contenu de dossiers.

De plus nous avons pu rédiger, voir et comprendre ce qu'était et impliquait une charte informatique, une charte de qualité ainsi que celle de confidentialité.

Enfin, nous avons pu nous sensibiliser quant à la nécessité de la sécurité informatique, de la criticité de la mise en place d'un plan de sauvegarde des données en entreprise tant dans le quotidien que dans le long terme.

Nous tenons également à remercier tous les intervenants du CESI REIMS, pour leurs aides et leurs conseils tout au long de la conception de ce projet.

XI. Conclusion

4Bits corporation s'engage donc à assurer vos besoins d'infogérance comme établi lors de ce rapport. Nous nous engageons également sur un comportement professionnel et exemplaire de la part de nos techniciens, ainsi que du respect des services attendu de leurs parts.

Nous assurons la bonne communication entre nos deux entreprises tant pendant les formations que pendant les interventions et la hotline mise en place grâce à « Customer Care ».

12. Annexe de la charte informatique

DISPOSITIONS LEGALES APPLICABLE

- Loi 91-646 du 10 juillet 1991 relative au secret des correspondances et des communications téléphoniques
- Loi N° 78-17 du 6 janvier 1978 informatique, fichier liberté
- Loi N° 78-753 du 17 juillet 1978 sur l'accès aux documents administratifs
- Loi N° 85-660 du 3 juillet 1985 sur la protection des logiciels
- Loi N° 88-19 du 5 janvier 1988 relative à la fraude informatique
- Loi N° 92-597 du 1er juillet 1992 relative au Code de la Propriété intellectuelle. Les recommandations de la CNIL du 28 mars 2001 et du 5 février 2002
- Article L122-5 L 111.1 du Code de la Propriété intellectuelle

XIII. Mémo Interne

Note interne à l'attention du personnel de 4Bits Corporation.
Pour donner suite aux retours d'enquête de satisfaction 4Bits tient à vous faire lire et approuver ce mémo.

- Tenue vestimentaire :

Une tenue vestimentaire correcte est exigée, lorsque vous effectuez une intervention sur un site vous représentez l'image de marque de l'entreprise ainsi que son sérieux, il est donc important de soigner votre apparence pour ne porter préjudice ni à l'entreprise ni aux clients.

- Ponctualité :

Tout le personnel est prié de se présenter à l'heure et de respecter les délais, en cas de retard ou d'imprévu, il est prié d'informer le client et de lui proposer un délai convenable pour ne pas lui porter préjudice.

- Comportement :

Tout le personnel doit avoir une posture professionnelle, il est donc demandé de s'exprimer correctement avec le client et de ne pas utiliser un langage familier.

- Respect du règlement :

Il est interdit d'utiliser des outils ou logiciels autres que ceux fournis par l'entreprise, vous ne devez donc ni lire, ni copier les fichiers d'un autre utilisateur. Si ces derniers ne sont pas dans l'espace public, il vous faut une autorisation verbale et écrite.

- Étapes à respecter :

Après chaque intervention il est nécessaire de faire un compte rendu auprès du client, avec un vocabulaire simple et clair qui ne soit pas trop « technique ».

Vous devez respecter le cahier des charges, si une demande qui n'y est pas inscrite est faite, demander auprès de la hiérarchie du client si cette demande est justifiée.
Vous devez vérifier le bon fonctionnement avant de débuter une autre tâche, si un problème est trop complexe demander de l'aide auprès de sa hiérarchie.

Si un équipement est endommagé et nécessite un remplacement, il est demandé de bien écouter la demande du client pour lui proposer une solution convenable.

Prénom, Nom lu et approuvé le……

XIV. Webographie

- http://www.ausimaroc.com/wp-content/uploads/2017/06/LMPS-AUSIM-Livre-Blanc-Classification-des-Donn%C3%A9es.pdf
- https://www.askabox.fr/liste-545-TN65hEJp8Ct.html
- https://www.olfeo.com/fr/solutions/filtrage-web
- https://certification.afnor.org/nos-solutions-en-securite-numerique
- https://qualite.ooreka.fr/comprendre/charte-qualite
- https://www.cnil.fr/fr/securite-informatique-sensibiliser-les-utilisateurs
- http://www.axone-group.com/service-informatique-externaliser
- https://www.data.gouv.fr/fr/datasets/correspondants-informatique-et-libertes-cil/
- https://www.cnil.fr/fr/definition/correspondant-informatique-et-libertes