

Etude de projet

Externalisation de la gestion du
parc informatique de
l'entreprise AutoConcept



Par Prest'Info : **PREST'INFO**

Table des matières

1. Notre entreprise	2
2. Votre projet	2
3. Charte informatique.....	3
4. Plan de sécurisation des données	4
4.1 Mot de passe.....	4
4.2 Modalité de communication aux utilisateurs et de mise en œuvre	4
4.3 Sauvegardes	4
4.4 Mise en œuvre des sauvegardes	5
4.5 Localisation des sauvegardes.....	5
4.6 Sauvegarde différentielle.....	7
4.7 Sauvegarde complète	7
5. Charte « Qualité Service Client »	8
6. Mémo interne.....	9
Annexes	10
Charte informatique.....	11
Article 1 : Utilisateurs concernés	11
Article 2 : Périmètre du système d'information.....	11
Article 3 : Règles générales d'utilisation	11
Article 4 : Sécurité informatique	12
4.1 Principe général de responsabilité et obligation de prudence	12
4.2 Obligation générale de confidentialité	12
4.3 Mot de passe.....	12
4.4 Verrouillage de sa session	13
4.5 Installation de logiciels	13
4.6 Copie de données informatiques	13
Article 5 : Accès à Internet	13
Article 6 : Email	13
Article 7 : Téléphonie	13
Article 8 : Sanctions	14
Article 9 : Information et entrée en vigueur	14
Charte « Qualité Service Client ».....	15
La continuité des services en cas de panne	15
Définition de la priorité	17
La relation client.....	17
La sécurité et la productivité	18
Mémo Interne.....	19

1. Notre entreprise

La société Prest'Info fournit des prestations de maintenance informatique complètes. Nous utilisons des outils de gestion des tickets pour vous permettre de gérer et de suivre vos demandes d'intervention. Nous utilisons également des outils de supervision et de monitoring pour surveiller en temps réel le bon fonctionnement de vos systèmes informatiques.

Afin d'étudier vos besoins et de maintenir votre parc informatique de manière performante, nos équipes procèdent dans un premier temps à un audit.

Nous évaluons votre matériel, vos solutions logicielles, votre réseau et son niveau de sécurité. A l'issue de ce diagnostic, nos équipes vous rendent un rapport d'instructions à suivre pour optimiser au mieux votre parc informatique.

Nos équipes sont présentes pour vous aider à faire les meilleurs choix pour vos solutions informatiques. Nous vous accompagnons pour l'achat, la mise en place, la migration ou le déploiement de solutions. Seul interlocuteur auprès de vos fournisseurs informatiques, nous gérons pour vous le SAV de tous ces intervenants.

Nous vous offrons un service d'assistance téléphonique afin de résoudre les problèmes liés à l'utilisation de vos solutions informatiques par l'ensemble de vos collaborateurs. Pour tout problème qui nécessite un déplacement de nos équipes techniques, nous intervenons chez vous dans des délais très courts.

Pour assurer la disponibilité permanente de vos applicatifs, nous assurons la maintenance de vos serveurs par supervision à distance : gestion des droits utilisateurs, paramétrage de votre messagerie, administration du domaine et de votre réseau, gestion des impressions.

2. Votre projet

Dans le but d'améliorer la qualité de service de votre système informatique vous nous avez mandaté afin que nous réalisions une étude concernant l'externalisation de la gestion de votre parc informatique. Celle-ci s'appuiera sur le cahier des charges que vous nous avez fourni, ci-dessous résumé :

1. Réalisation d'une charte informatique synthétique mettant l'accent sur ce que la loi autorise ainsi que ce qu'il est possible aux utilisateurs de faire. Nous détaillerons les points suivants :
 - Les règles qui régissent l'utilisation des moyens informatiques mis à disposition des salariés,
 - Les moyens à mettre en œuvre pour la sécurité des fichiers,
 - Les informations qui doivent être portées aux personnes dans l'entreprise concernant l'utilisation des outils informatiques,
 - Les dispositions légales concernant la mise en place d'une solution de filtrage de contenus en entreprise.
2. Etablissement d'un plan de sécurisation des données porté sur :
 - La politique de sécurité des mots de passes et les modalités de communication aux utilisateurs,

- Les mesures immédiates de sauvegarde.
3. Rédaction d'une charte « Qualité Service Client » qui insistera sur :
- La continuité de service en cas de panne,
 - Le relationnel client,
 - La sécurité et la productivité.
4. Création d'un mémo interne à transmettre aux salariés ainsi qu'aux nouveaux arrivant édictant la conduite à tenir des techniciens chez un client.

3. Charte informatique

Afin de répondre au mieux à vos attentes nous avons établi une charte informatique que vous trouverez en annexe.

Celle-ci sera à adjoindre au règlement intérieur de votre entreprise et à faire émarger par l'ensemble de vos salariés. Elle fixe les dispositions légales qui régissent l'utilisation d'un service d'information ainsi que les droits et devoirs de chaque utilisateur.

Les solutions de filtrages et de suivis qui seront mises en place sont des obligations légales. En effet l'obligation de mettre en place des filtres et de conserver pendant un an les données de connexion, imposée aux fournisseurs d'accès Internet (FAI) par l'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) a été étendue à tous ceux qui offrent un accès à l'internet selon la loi antiterroriste du 23 janvier 2006.

De plus, l'article L.34 du Code des postes et des communications électroniques (CPCE), complété par la loi relative à la lutte contre le terrorisme (2006), dispose que :

"Les personnes qui, au titre d'une activité professionnelle [...] offrent au public une connexion permettant une communication en ligne [...], y compris à titre gratuit, sont soumises au respect des dispositions applicables aux opérateurs de communications électroniques". ([Source : Olfeo](#))

Le filtrage permet également de veiller à ce que l'accès internet fourni par l'entreprise ne permette pas de contrevenir aux droits de propriété intellectuelle par un téléchargement illégal d'œuvres protégées par le droit d'auteur. (Loi Hadopi)

Pour que ces solutions de filtrages soient conformes à la loi 3 grands principes doivent être respectés :

- Les droits des personnes
- La déclaration à la CNIL
- La sécurisation des données collectées

Les personnes dont les données à caractère personnel font l'objet d'un traitement automatisé des données doivent être informées (mention dans la charte informatique). Elles doivent également être en mesure d'exercer leur droit de rectification, d'interrogation et d'accès aux données collectées conformément à l'article 39 de la loi Informatique et Liberté.

Dès lors que le dispositif de filtrage permet un contrôle individuel, celui-ci doit faire l'objet d'une déclaration auprès de la CNIL.

Enfin, le principe de sécurité et de confidentialité des données prévoit une obligation de sécurité des données traitées à caractère personnel.

4. Plan de sécurisation des données

4.1 Mot de passe

Chaque mot de passe doit obligatoirement être modifié selon la fréquence suivante : 6 Mois. Un mot de passe doit, pour être efficace, comporter 12 caractères alphanumériques. Il ne doit pas être identique au login, comporter le nom et/ou le prénom de l'utilisateur ou de membres de sa famille, le numéro de téléphone, la marque de la voiture ou toute référence à quelque chose appartenant à l'utilisateur, être un mot ou une liste de mots du dictionnaire ou un nom propre, nom de lieu, être écrit sur un document et être communiqué à un tiers.

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 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.

4.2 Modalité de communication aux utilisateurs et de mise en œuvre

Lors de l'arrivée d'un nouveau collaborateur nous lui fournirons un identifiant (nom, prénom) ainsi qu'un mot de passe provisoire. A sa première connexion il devra changer son mot de passe en respectant la politique de mot de passe de l'entreprise. Ces informations seront communiquées au moyen d'une fiche « Nouvel arrivant » qui contiendra ses identifiant de connexion, son adresse mail et les mots de passes temporaires associés.

4.3 Sauvegardes

Tous les utilisateurs doivent sauvegarder les fichiers sur leurs postes, selon la priorité des données et de la place occupée dans l'entreprise, une sauvegarde de son poste sera effectuée plus ou moins régulièrement, cette sauvegarde du poste permet de récupérer des données effacées ou détruites par erreur, ou volontairement, par des salariés.

Le formatage du disque dur du poste de travail infecté et la restauration des données sont en effet la seule solution véritablement efficace contre ce type d'attaque.

Elles facilitent le redémarrage de votre activité après un dégât des eaux ou un incendie. Toutes vos données professionnelles sont importantes.

Mais certaines présentent une importance capitale : brevets, fichiers clients et prospects, factures, documents administratifs et tous ceux intégrant des données à caractère personnel.

La sauvegarde des intérêts nécessite le respect d'une obligation générale et permanente de confidentialité et de secret professionnel, à l'égard des données disponibles mis à la disposition de l'utilisateur pour l'exercice de son activité professionnelle dans le cadre notamment de l'utilisation des systèmes d'information, mais aussi de tout traitement.

4.4 Mise en œuvre des sauvegardes

Selon le poste la sauvegarde sera différente il y a 2 types de sauvegarde que nous utilisons la complète et différentielle.

Pour la plupart nous effectuerons des sauvegardes différentielle, les données ajoutées ou modifiées seront sauvegardées sur le NAS de l'entreprise pour ensuite être stocker et envoyer sur le cloud.

Pour les sauvegardes différentielles celle-ci se dérouleront de 6h à 22h, une fois par semaine à 00h00 une sauvegarde complète de chaque poste sera effectuée, et 1 fois par mois une sauvegarde complète sera gardée 12 mois sur le cloud.

Pour la société AutoConcept nous allons effectuer des sauvegardes incrémentales journalière : Pour l'atelier, les pièces de rechange et la vente, des sauvegardes seront effectuées tous les soirs à 22h. Pour la comptabilité toute les 2 heures car la perte de ces données ne sont pas acceptables et pour la direction nous ferons 3 sauvegardes par jour : 8h00 - 12h00 - 22h00.

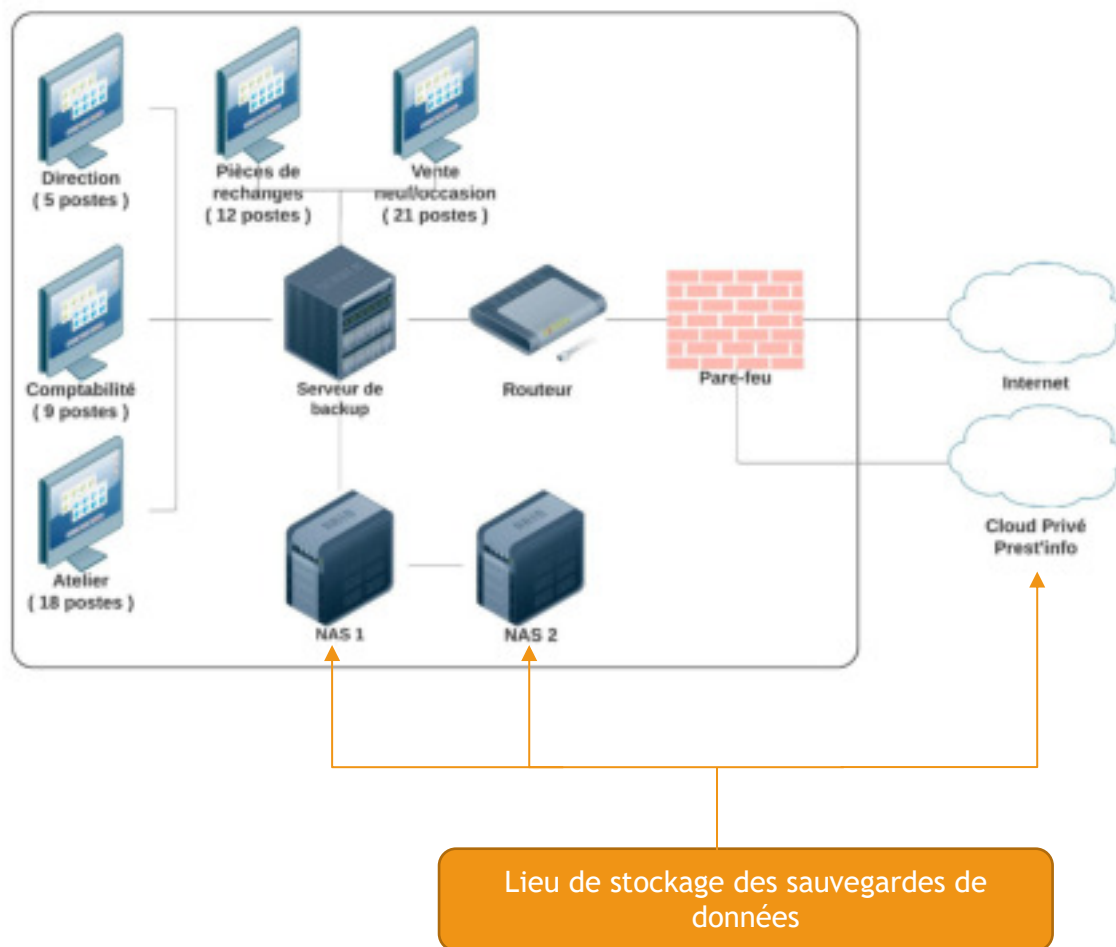
Toutes les semaines nous effectuerons une sauvegarde complète de chaque poste, elle sera effectuée à 00h00 le samedi soir.

4.5 Localisation des sauvegardes

Après avoir repéré leur lieu exact de stockage (serveur, Cloud, prestataire local, etc.), il est indispensable de les classer par ordre d'importance selon une échelle de 1 à 5, 1 étant « insignifiant » et 5 « catastrophique ». Toutes celles qui ont 4 au minimum doivent bénéficier d'une sécurité renforcée : authentification et surveillance des accès, chiffrement, sauvegardes régulières. Tous ces sauvegardes seront placer sur 2 Nas que nous vous fournirons. Les 2 auront exactement le même contenu, une fois par semaine une copie du Nas sera envoyée nôtre cloud privé pour garder une sauvegarde en dehors du site d'activité.

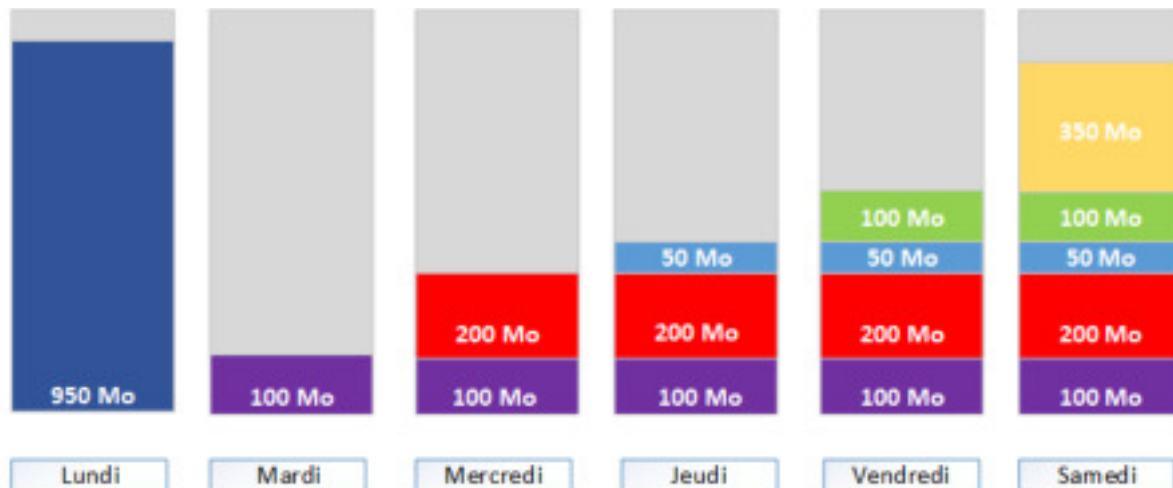
Jour	Type de sauvegarde
Lundi	Sauvegarde différentielle
Mardi	Sauvegarde différentielle
Mercredi	Sauvegarde différentielle
Jeudi	Sauvegarde différentielle
Vendredi	Sauvegarde différentielle
Samedi	Sauvegarde Complète

DIAGRAMME RÉSEAU AUTOCONCEPT



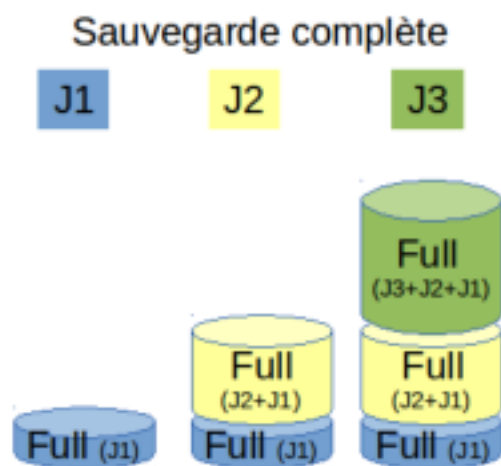
4.6 Sauvegarde différentielle

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. Par ailleurs, le principal avantage de cette catégorie de sauvegarde est qu'il est entièrement fiable étant donné qu'il ne suffira que de la sauvegarde complète pour reconstituer toutes les données sauvegardées.



4.7 Sauvegarde complète

La sauvegarde complète permet de sauvegarder toutes les données, les répertoires et les sous répertoires sélectionnés. C'est le type de sauvegarde le plus rapide, le plus simple, et le plus précis pour restaurer les données sans erreurs. Cependant, les sauvegardes complètes prennent beaucoup de temps pour de gros volumes de données, elles ne sont pas effectuées quotidiennement car elle serait trop longue à réaliser. Généralement, les sauvegardes complètes sont effectuées le samedi soir (ou la veille d'un jour où l'entreprise ne travaille pas) pour ne pas gêner l'activité de l'entreprise. Pour pouvoir sauvegarder les données au fur et à mesure de leurs modifications sans pour autant faire des sauvegardes complètes chaque jour, notre entreprise utilise des sauvegardes différentielles.



5. Charte « Qualité Service Client »

La mise en place et l'utilisation de technologies de l'information a un impact sur la vie professionnelle des utilisateurs. Le respect des personnes est une valeur fondamentale pour nos intervenants et il nous importe de mettre en œuvre les moyens permettant d'éviter de nuire aux clients et collaborateurs de l'entreprise.

Ce respect doit également se traduire dans les relations entre les membres du service informatique et les collaborateurs des autres services afin de partager les connaissances et ainsi maintenir une ambiance et une efficacité de travail optimal.

Dans cet optique nous vous proposons la charte « Qualité Service Client » que vous trouverez en annexe. Celle-ci a pour but de définir les bonnes pratiques d'utilisations du système d'information.

Afin de garantir un service de qualité nous nous basons sur la démarche ITIL :

Qu'est-ce que la démarche ITIL ?

ITIL (« Information Technology Infrastructure Library » pour « Bibliothèque pour l'infrastructure des technologies de l'information ») est l'ensemble d'ouvrages recensant les bonnes pratiques du management du système d'information. C'est un référentiel méthodologique très large qui aborde les sujets suivants :

- Comment organiser un système d'information ?
- Comment améliorer l'efficacité du système d'informatique ?
- Comment réduire les risques ?
- Comment augmenter la qualité des services informatiques ?

L'adoption des bonnes pratiques ITIL présente de nombreux avantages. Les normes ITIL sont des normes de qualités préétablies au niveau international. Les bonnes pratiques ITIL pourraient être apparentées à un **label de qualité**.

La préoccupation principale de ses normes est la traçabilité. Faire appel à une entreprise de services numériques qui met en place les pratiques de la norme ITIL vous assure une entière transparence des actions menées sur votre parc informatique.

L'objectif d'ITIL est de vous assurer un niveau de qualité optimum pour votre système d'information et une expérience utilisateur satisfaisante. ([Source : Wikipédia](#))

6. Mémo interne

Afin de définir un cadre d'intervention professionnel de nos techniciens, nous avons rédigé un mémo interne à destination de ceux-ci. Il nous permettra de vous garantir que nos techniciens adoptent la bonne attitude et qu'ils n'interfèrent pas dans le bon fonctionnement de vos services.

S'il devait toutefois y avoir des écarts de comportement de nos techniciens, nous vous invitons, par le billet du formulaire de contact que nous vous fournirons de nous en informer dans les meilleurs délais. Cela nous permettra d'intervenir, dans le but de garder une qualité de service optimale.

Annexes

Charte informatique

Article 1 : Utilisateurs concernés

La présente charte s'applique à l'ensemble des utilisateurs du système d'information dont notamment :

- Les dirigeants et mandataires sociaux
- Les salariés
- Les intérimaires
- Les stagiaires
- Les employés de sociétés prestataires
- Les visiteurs occasionnels

Il appartient aux salariés de l'organisation de s'assurer de faire accepter la présente charte à toute personne à laquelle ils permettraient l'accès au SI.

Article 2 : Périmètre du système d'information

Le système d'information est composé des ressources suivantes :

- Ordinateurs
- Téléphones
- Réseau informatique (serveurs, routeurs et connectique)
- Photocopieurs
- Logiciels
- Données informatisées
- Messagerie
- Smartphones, tablettes

Aux fins d'assurer la sécurité informatique du SI, tout matériel connecté au SI de l'entreprise, y compris le matériel personnel des utilisateurs indiqués à l'article 1, est régi par la présente charte.

Article 3 : Règles générales d'utilisation

Le SI doit être utilisé à des fins professionnelles, conformes aux objectifs de l'organisation, sauf exception prévue par les présentes, ou par la loi.

Les utilisateurs ne peuvent en aucun cas utiliser le SI de l'organisation pour se livrer à des activités concurrentes, et/ou susceptibles de porter préjudice à l'organisation de quelque manière que ce soit.

Article 4 : Sécurité informatique

L'entreprise met en œuvre une série de moyens pour assurer la sécurité de son système d'information et des données traitées, en particulier des données personnelles. A ce titre elle peut limiter l'accès à certaines ressources.

4.1 Principe général de responsabilité et obligation de prudence

L'utilisateur est responsable des ressources informatiques qui lui sont confiées dans le cadre de ses missions, et doit concourir à leur protection, notamment en faisant preuve de prudence. L'utilisateur doit s'assurer d'utiliser les ressources informatiques mises à sa disposition de manière raisonnable, conformément à ses missions.

4.2 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, et en particulier des données personnelles, traitées sur le SI de l'organisation.

Il s'engage à prendre toutes les précautions utiles pour éviter que ne soient divulguées de son fait, ou du fait de personnes dont il a la responsabilité, ces informations confidentielles.

4.3 Mot de passe

L'accès aux SI ou aux ressources informatiques mises à disposition est protégé par mot de passe individuel. Ce mot de passe doit être gardé confidentiel par l'utilisateur afin de permettre le contrôle de l'activité de chacun. Le mot de passe doit être mémorisé et ne doit pas être écrit sous quelque forme que ce soit. Il ne doit pas être transmis ou confié à un tiers ou être rendu accessible. Le login et le mot de passe doivent être saisis lors de chaque accès au système d'information.

Le mot de passe doit se conformer à la politique de mot de passe édictée, conformément [aux prescriptions de la CNIL](#) relatives à la protection des données personnelles et notamment :

- Être composé de plus de 12 caractères ;
- Ces caractères doivent être une combinaison de caractères alphanumériques,
- De chiffres,
- De majuscules,
- De minuscules,
- Et de caractères spéciaux

Celui-ci devra être renouvelé au minimum tous les 6 mois.

4.4 Verrouillage de sa session

L'utilisateur doit veiller à verrouiller sa session dès lors qu'il quitte son poste de travail.

4.5 Installation de logiciels

L'utilisateur ne doit pas installer, copier, modifier ou détruire de logiciels sur son poste informatique sans l'accord du service informatique en raison notamment du risque de virus informatiques.

4.6 Copie de données informatiques

L'utilisateur doit respecter les procédures définies par l'organisme afin d'encadrer les opérations de copie de données sur des supports amovibles, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité, afin d'éviter la perte de données (ex : vol de clé USB, perte d'un ordinateur portable contenant d'importantes quantités d'informations confidentielles...).

Article 5 : Accès à Internet

L'accès à l'Internet est autorisé au travers du SI, toutefois, pour des raisons de sécurité ou de déontologie, l'accès à certains sites peut être limité ou prohibé par la direction informatique qui est habilitée à imposer des configurations du navigateur et à installer des mécanismes de filtrage limitant l'accès à certains sites, ainsi que d'enregistrer les logs d'utilisation d'Internet. Seule la consultation de sites ayant un rapport avec l'activité professionnelle est autorisée.

Bien sûr, il est interdit de se connecter à des sites Internet dont le contenu est contraire à l'ordre public, aux bonnes mœurs ou à l'image de marque de l'entreprise, ainsi qu'à ceux pouvant comporter un risque pour la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci.

Article 6 : Email

Chaque employé peut disposer d'une adresse email pour l'exercice de ses missions.

Par principe, tous les messages envoyés ou reçus sont présumés être envoyés à titre professionnel.

Par exception, les utilisateurs peuvent utiliser la messagerie à des fins personnelles, dans les limites posées par la loi. Les messages personnels doivent alors porter la mention "PRIVE" dans l'objet et être classés dans un répertoire "PRIVE" dans la messagerie, pour les messages reçus.

Toutefois, les utilisateurs sont invités, dans la mesure du possible, à utiliser leur messagerie personnelle via un client en ligne pour l'envoi de messages à caractère personnel plutôt que la messagerie de l'entreprise.

Article 7 : Téléphonie

Pour leur activité professionnelle, les utilisateurs peuvent disposer d'un poste fixe et d'un terminal mobile, smartphone, tablette ou clé 3G.

Pour ce qui est de l'utilisation des terminaux mobiles en connexion pour accès à des sites Internet ou à la messagerie électronique, les règles édictées ci-dessus s'appliquent de la même manière. De plus, il est rappelé que l'envoi de SMS est réservé aux communications professionnelles et qu'il engage la responsabilité de l'émetteur au même titre que l'envoi d'un courriel.

Il est donc soumis aux mêmes règles rappelées plus haut. Enfin, les connexions depuis l'étranger sont strictement interdites sauf autorisation exceptionnelle de la hiérarchie en cas d'urgence professionnelle.

Article 8 : Sanctions

Les manquements aux règles édictées par la présente charte peuvent engager la responsabilité de l'utilisateur et entraîner des sanctions à son encontre (limitation d'usage du SI, sanctions disciplinaires).

Article 9 : Information et entrée en vigueur

La présente charte est ajoutée en annexe du règlement intérieur et communiquée individuellement à chaque employé.

Elle entre en vigueur au [date d'adoption de ladite charte]

Charte « Qualité Service Client »

La continuité des services en cas de panne

Lors de la demande de support :

Le logiciel mis en place (GLPI) sera utilisé afin de créer un système de ticket (demande ou incident) qui sera rédigé par le technicien sur place après qu'il est été sollicité par l'utilisateur, afin d'organiser les demandes par ordre d'urgence et de traitement. Par ce système il sera indiqué à l'utilisateur tous les détails du suivi et du traitement.

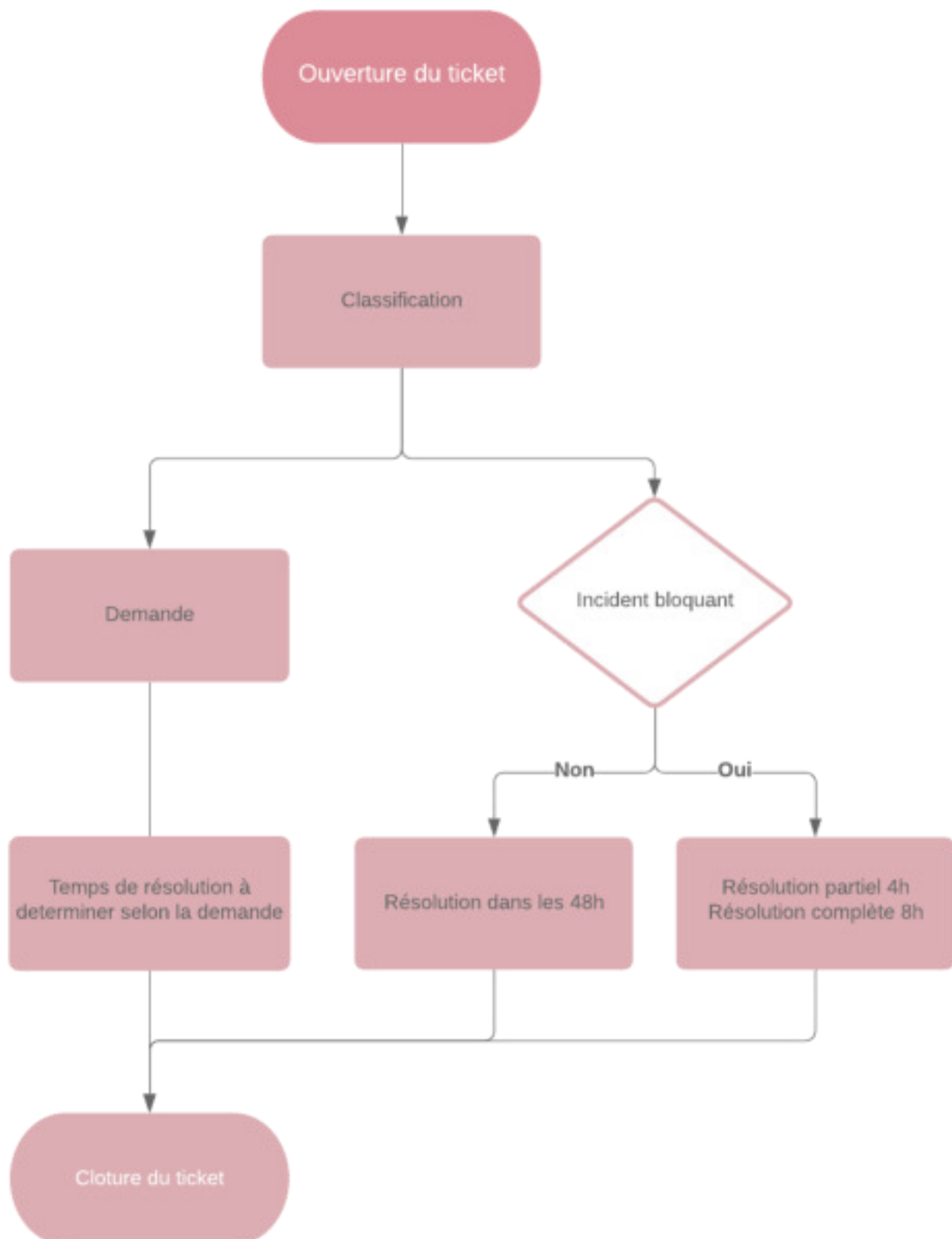
Afin de créer un ticket, l'utilisateur aura plusieurs moyens pour prendre contact avec le support :

- Par téléphone au 123 (numéro unique et non surtaxer).
- Par mail : support@prestinfo.com

Chaque utilisateur sera identifié afin de garantir le dépannage sur le matériel associé. La demande où l'incident sera d'abord analysé par le support niveau 1 (technicien présent sur site), si nécessaire le technicien du support niveau 1 pourra alors faire une demande de prise en charge au support niveau 2 (Prest'Info) qui répondra à la demande de l'utilisateur.

L'urgence de la demande ou de l'incident sera identifiée afin de déterminer si le dysfonctionnement est bloquant pour l'utilisateur. En cas de dysfonctionnement bloquant nous nous engageons à intervenir dans un délai maximum de 4H pour un rétablissement partiel et 8h pour un rétablissement complet

Algorithme gestion ticket



Définition de la priorité

Afin de définir si un incident est bloquant et pour leur bonne gestion, Prest'Info met en place une échelle de priorité basée sur l'impact et l'urgence.

IMPACT (sur le travail et la productivité d'AutoConcept)

Fort	Incident générique qui impacte plusieurs utilisateurs.
Moyen	Incident isolé qui impacte un seul utilisateur.
Faible	Evènement ou incident sans impact et non bloquant

URGENCE

Haute	L'utilisateur ne peut pas travailler
Moyenne	L'utilisateur peut encore travailler mais en mode dégradé
Faible	L'utilisateur peut encore travailler

La priorité est calculée sur la base de l'impact et de l'urgence pour l'utilisateur. Ce calcul sert à identifier les délais acceptables dans la mise en œuvre d'une action. La détermination d'un code de priorité permet de traiter l'incident par l'outil et le personnel nécessaire.

Un rapport statistique des services de gestion de ticket sera transmis chaque mois au directeur général.

La relation client

Le technicien s'engage à offrir un accueil personnalisé pour chaque utilisateur, s'impliquer en employant un ton dynamique, chaleureux et accueillant. Il s'engage à agir avec politesse, discrétion et respect de la vie privée. Le technicien se doit de répondre aux besoins des utilisateurs et leur fournir des services de qualité adaptés à leurs besoins ou attentes.

Pour les nouveaux collaborateurs de l'entreprise AutoConcept, une fiche personnalisée sera remise au même moment que son matériel informatique. Elle aura pour but d'expliquer sans terme technique les accès, l'utilisation des outils et logiciels informatiques mis à disposition de celui-ci.

Une formation de 45 min sera réalisée lors de la remise du matériel avec un technicien afin de faire ensemble le point sur les outils et les techniques d'utilisations.

Pour garantir une meilleure communication entre le service informatique et les utilisateurs, un logiciel de suivi des traitements (GLPI) est mis en place afin de pouvoir communiquer des informations relatives au dépannage à effectuer. L'utilisateur sera observateur de son ticket et aura la possibilité d'interagir avec le technicien.

L'utilisateur aura également la possibilité de téléphoner aux techniciens afin qu'ils trouvent des solutions directes, qu'ils fassent de la prise en main à distance et qu'ils créent un ticket pour traiter la demande.

De la documentation sur le fonctionnement de l'informatique générale et le fonctionnement des logiciels sont également consultable par l'utilisateur qui souhaite s'informer sur l'utilisation de ses outils informatiques. La base de connaissances de GLPI sera également accessible.

Le technicien se doit de tenir informé l'utilisateur sur les techniques de sauvegardes, l'avancée de la résolution des incidents et les temps de maintenances.

Afin de diminuer le nombre d'incident, le support mettra en place une démarche ITIL qui sera alimentée par des process et qui auront pour but d'aider les utilisateurs dans leur quotidien face aux utilisations des outils informatiques.

Cette démarche aura également pour but :

- La satisfaction des utilisateurs ;
- L'amélioration de la communication inter-service ;
- Un niveau de sécurité optimal ;

A la clôture du ticket incident l'utilisateur aura la possibilité de répondre à un questionnaire de satisfaction constitué de 3 points important :

- Évaluation de la qualité de traitement de la demande ;
- Évaluation de la durée du traitement ;
- Évaluation de la qualité de l'accueil.

Un cadre réservé sera à disposition afin de déposer un commentaire, une suggestion ou tous autres éléments que l'utilisateur jugerait utile d'inscrire.

Il est recommandé à l'utilisateur de répondre à ce questionnaire, ceci afin d'améliorer la qualité des services proposés. Un rapport mensuel sera transmis au directeur général afin de faire le point sur les éléments que nous pourrions encore améliorer.

La sécurité et la productivité

L'informatique est indispensable à l'activité d'une entreprise. Elle a pour but d'améliorer la productivité en entreprise.

Tout utilisateur de l'entreprise disposera après décision de son responsable hiérarchique d'un ordinateur adapté à sa fonction.

Il pourra également disposer d'un téléphone portable. Ce matériel sera configuré par le technicien informatique avec les logiciels et programmes dont l'utilisateur aura besoin. Si l'utilisateur voit ses fonctions changer ou évoluer il pourra demander au technicien d'adapter son matériel à sa nouvelle fonction ou évolution.

En cas de panne de son matériel, la mise à disposition de matériels informatiques de remplacement sera garantie. L'utilisateur aura ainsi la possibilité de poursuivre son travail sur un poste de prêt en utilisant son identifiant et ses mots de passe de session Windows, lui permettant de rester productif durant le dépannage de son matériel.

Afin de garantir une sécurité informatique au sein de l'entreprise, l'utilisateur ne sera pas administrateur de son poste, aucun programmes/logiciels ne pourra être installé. L'utilisateur aura la possibilité de demander l'installation d'outils au technicien, celui-ci sera en mesure de vérifier les sources du programme/logiciel et d'installer l'outil demandé si celui-ci répond aux normes de sécurité ainsi qu'au besoin opérationnel de l'entreprise. (Voir [art 4.5](#) de la charte informatique).

Pour des raisons de sécurités et de confidentialités l'utilisateur ne devra pas fournir ses mots de passe, ceux-ci étant strictement confidentiel. Aucun technicien ne sera disposé à demander ses informations à l'utilisateur. (Voir [art. 4.3](#) de la charte informatique)

L'utilisateur aura le devoir de sauvegarder ses fichiers et documents sur un disque prévu à cet effet. Une formation utilisateur sera proposée afin qu'il prenne connaissance de la manipulation à réaliser.

Mémo Interne

Objet : Conduite à tenir chez un client

Destinataire : Techniciens informatique Prest'Info.

- Le technicien devra adopter une tenue correcte et professionnelle lors d'une intervention chez un client. Il évitera les tenues trop décontractées (jogging, short, bermuda, claquette...)
- Lors d'un déplacement chez un client, si le technicien a un retard ou un empêchement il sera tenu d'informer celui-ci.
- Le technicien veillera à employer un langage compréhensible, courtois et évitera les termes trop techniques.
- Le technicien tachera d'expliquer clairement les actions mener sur le poste du client.
- Le technicien aura le devoir de conseiller et de former le client sur la bonne utilisation de ses outils informatiques.
- En cas de conflit avec un client, le technicien en réfèrera à sa direction afin de résoudre le dit conflit.
- Le technicien s'assurera que le poste du client est effectivement réparé avant d'effectuer son retour.
- Lorsqu'une intervention urgente est planifiée, le technicien se doit de l'honorée. Si un cas de force majeur devait l'empêcher d'intervenir, il avertira l'utilisateur de son empêchement et tachera de faire passer cette intervention en priorité après s'être libéré.
- Le technicien fera preuve de discrétion, il sera tenu au secret professionnel et ne portera pas atteinte à la vie privée du client.
- Le technicien portera une attention particulière aux attentes du client et l'informeront si son matériel ne peut être remplacé à l'identique.
- Le technicien sera tenu d'informer le client sur l'avancer de son incident ou de sa demande.
- Lors d'un appel téléphonique, le technicien devra faire preuve de courtoisie et apporter assistance au client.
- L'ouverture d'un ticket est indispensable même en cas de résolution immédiate par téléphone.
- Le technicien mettra à jour régulièrement les tickets afin d'informer le client sur l'évolution de sa demande ou de l'incident.