3 décembre 2019

Projet SAS

GEOFFROY Chloé – BAUER Alexandre – ANTOINE Baptiste
SYSTEM NET CORP

Table des matières

Objectifs du Projet SAS

Le projet SAS est un premier projet visant à nous faire acquérir les comportements appropriés du technicien système et réseau en entreprise.

L'identification des mesures réglementaires gérant la mise en place de l'informatique dans l'entreprise est également un des objectifs primordiaux de notre métier.

Après ce projet, nous devons être en mesure d'apporter des solutions rapides et efficaces à des problématiques entravant la production de biens ou de services de la société ainsi que de concevoir un dossier de synthèse des choix effectués, de communiquer dessus et de les défendre.

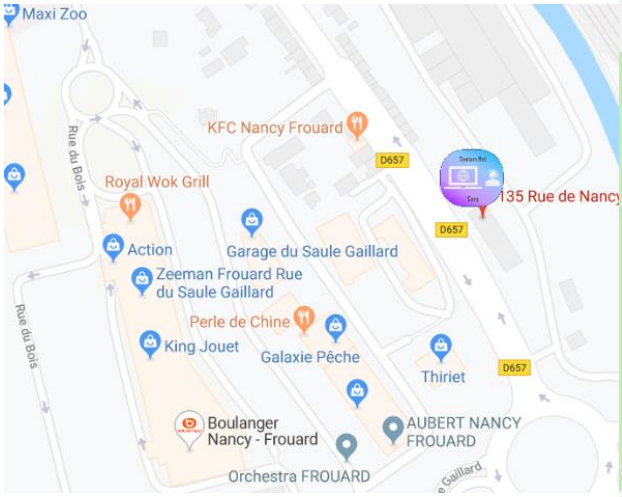
Création de notre entreprise prestataire :

Nom : System net Corp

Logo :

Situation géographique :

- Client : AutoConcept ZI St Jacques Maxéville
- Entreprise : 135 Rue de Nancy 54390 Frouard



Présentation de notre entreprise :

L'équipe technique de System Net Corp effectue l'intégration et le déploiement de solutions informatiques, d'impression, et serveurs pour les TPE/PME. Nous déployons des solutions logicielles et matérielles pour la sécurité de vos réseaux, données et accès à distance de votre infrastructure informatique. Nous proposons des solutions pour la continuité d'activité adaptées à toutes les TPE/PME.

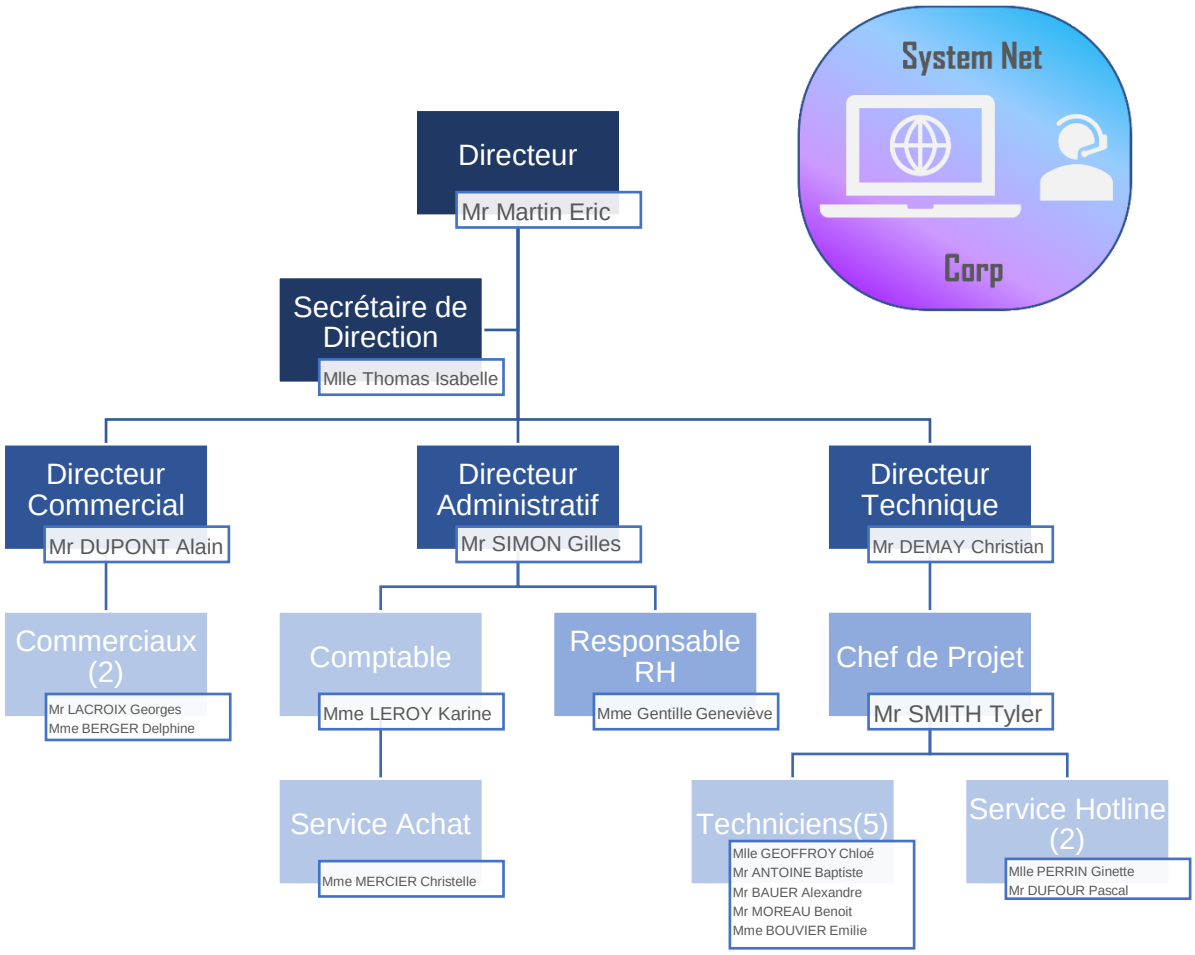
Nous veillons à tenir compte de votre actif informatique et de votre environnement métier, grâce à un audit de votre infrastructure, préalablement effectué. Nous sommes à l'écoute de vos besoins et vous proposons les solutions les mieux adaptées à votre type d'activité.

Nos services Helpdesk interviennent sur site, dans nos ateliers, et à distance, grâce à nos outils de télémaintenance sécurisés. Ceux-ci intègrent des actions correctives et préventives. Vous bénéficiez d'un support dédié en cas de dysfonctionnement de votre système. Notre service d'astreinte permet à nos clients sous contrat de bénéficier jour et nuit d'intervention en cas de besoin.

Notre proximité géographique, nous permet de nous engager sur des délais d'intervention rapides et de tout mettre en œuvre pour que le souci rencontré soit traité et résolu dans les 6 heures (pannes niveau 1 et 2). Notre support téléphonique est joignable 24/24 grâce à un service d'astreintes.

Les certifications et formations acquises par nos techniciens leurs permettent de maîtriser les dernières technologies afin de répondre au mieux aux besoins de nos clients. Nos commerciaux s'informent des dernières technologies afin de proposer les meilleures solutions répondant à vos critères.

Organigramme :



Les outils :

- Traitement de texte, partage de documents, conversation en groupe, restitution de la gestion de temps :

- Recherches sur internet :

- Mise en forme des images :

Charte graphique :

- ✓ **En-tête de page :**

- ✓ **Pied de page :**

- ✓ **Texte :**
  - Texte en « Arial »
  - Taille 11
  - Couleur personnalisée : rgb (88,88,88)

Étude de l'existant

Présentation d'AutoConcept :

AutoConcept est une concession automobile basée à Maxéville qui emploie environ 80 personnes. Cette société assure la vente de voitures et d'utilitaires neufs ou d'occasion, la vente de pièces détachées et la réparation de tous types de véhicules. Cette société fait appel à nous car elle souhaite externaliser son service informatique composé de 70 à 80 postes.

Étude de l'existant :

AutoConcept possède un parc informatique actuellement géré par deux informaticiens employés par la société. Depuis quelques temps, les plaintes des utilisateurs se sont accumulées. Ils ont remarqué que la qualité des services de ce service avait baissé, engendrant des pertes d'exploitation ainsi que des pertes économiques importantes.

Les problématiques rencontrées sur ce projet sont les suivantes :

- La société AutoConcept a choisi un amortissement de son matériel informatique sur 3 ans. Avant ce délai, le service comptabilité n'autorisera pas le changement de matériel.
- Les coûts minimums engendrés par un arrêt des activités par employé :

Temps d'arrêt du personnel	Coût brut de l'arrêt (€)	Coût avec charges (€)
1 heure	10	20
1 jour	75	150

- La récurrence de la lenteur des postes entraîne une perte de productivité qui peut aboutir sur une perte d'activité donc de bénéfices pour l'entreprise.
- Le comportement des techniciens actuels est inadapté. Il leur est surtout reproché un manque de professionnalisme lors de leur intervention (tenue non appropriée, matériel non restitué).
- Le service informatique actuel a accumulé les retards de traitement des tickets. Un manque de communication sur l'avancement des réparations est à déplorer.
- La confidentialité des données de l'entreprise et des utilisateurs a été mise à mal à plusieurs reprises.
- Un manque de sécurité du site avec des accès non contrôlés aux postes de travail a été constaté.
- La sécurité des mots de passe faibles voire absents met à mal la sécurité des données de l'entreprise.
- De nombreux utilisateurs se sont plaint au sujet du support téléphonique du service informatique. Certains de leurs problèmes ne sont pas traités, leurs logiciels ne possèdent pas de licences valides activées.

Problèmes concrets :

- Le crash du disque dur d'un poste commercial a causé une perte financière de 80000€.
- Le poste de travail en panne d'une secrétaire commerciale en SAV pendant 2 jours a entraîné une perte de 60000€. Un contrat n'a pas pu être finalisé à cause d'une perte d'activité.
- Un client s'est introduit sur un poste de travail dépourvu de mot de passe.
- Une demande d'intervention urgente qui était planifiée le lundi n'a été traitée que le mercredi.
- Le service comptabilité soupçonne un technicien informatique de consulter certaines de leurs données confidentielles et de les divulguer à des tiers.

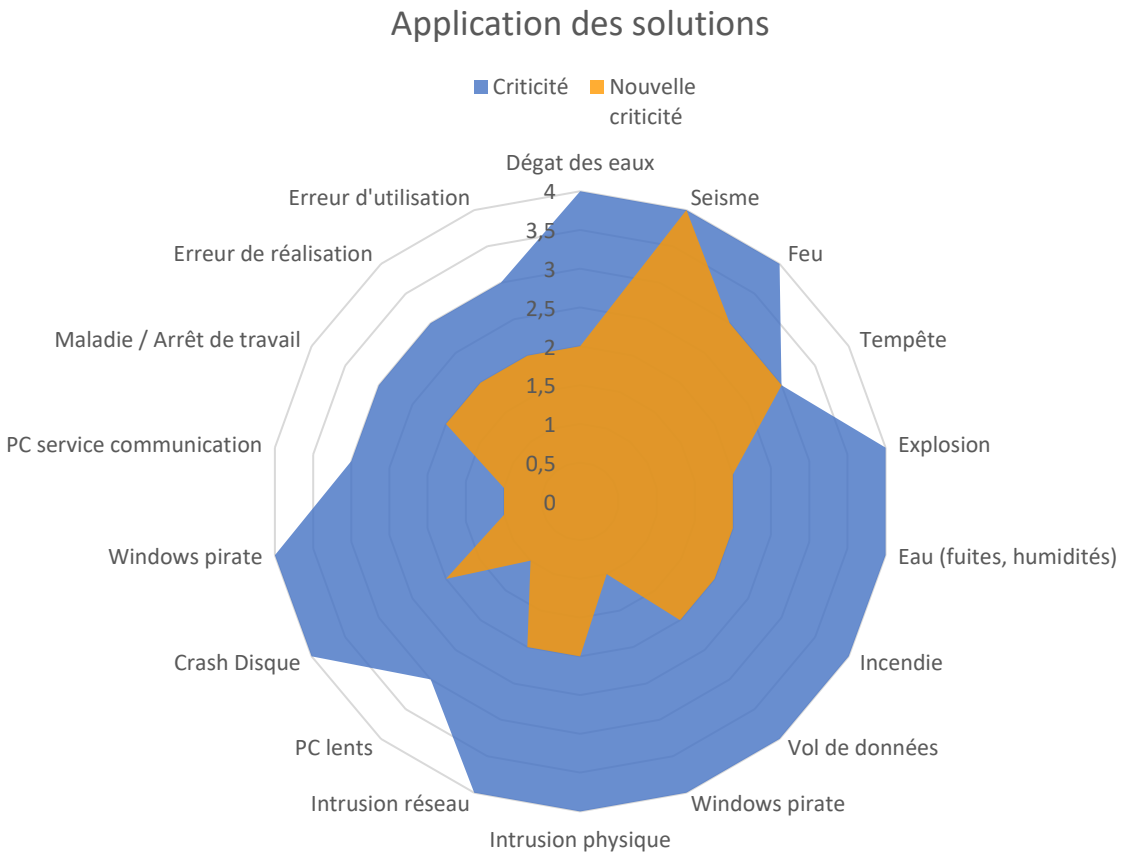
Besoins d'AutoConcept :

- Des moyens de sauvegarder les données des utilisateurs afin de reprendre une activité après une panne.
- Des solutions de stockage de fichiers tolérantes à la panne.
- Des moyens de sécurisation des données et d'accès aux postes de travail des employés.
- La formation du personnel utilisant le système d'information de l'entreprise.
- Le rappel des bonnes pratiques et des bons comportements aux employés du service informatique venant d'AutoConcept.

Études des risques :

Risques	Types	Probabilité	Criticité	Résultat	RESPONSABLE / INFLUENCE	SOLUTIONS POSSIBLES
Risques Naturels	Dégat des eaux	2	4	8	Crues Meurthe	PREVENTIVE : Salle serveur(création) surélevée, éviter les PC au sol
	Seisme	1	4	4		
	Feu	2	4	8	Foudre, criminel	PREVENTIVE : Mesures de sécurités, Argonite dans salle serveurs, surveiller végétation
	Tempête	2	3	6	Vents forts, bord de Meurthe	PREVENTIVE : Surveiller hauteur des arbres aux alentours de l'entreprise
Risques Explosion	Explosion	2	4	8	Huiles, carburants, vehicules	PREVENTIVE : Mesures de sécurités, assurances
	Eau (fuites, humidités)	2	4	8	Conduites, Climat régional	PREVENTIVE : Installer des capteurs d'humidité et d'eaux dans le faux plancher, assurances
	Incendie	2	4	8	Huiles, carburants, véhicules	PREVENTIVE:Mesures de sécurités, Argonite dans salle serveurs, assurances
Risques Malveillance	Vol de données	4	4	16	(Fichiers clients?)	CURATIVE : Sécurisation du réseau via mots de passes
	Windows pirate	3	4	12	Ancien service Info	CURATIVE : Réinstallation des postes clients et mesures de sécurité info
	Intrusion physique	4	4	16	Resp Atelier	CURATIVE : Sécuriser l'accès à l'atelier, au poste info du moins
	Intrusion réseau	3	4	12	Ancien service Info	CURATIVE : Protection des postes par Mot de passe
Défaillance Système	PC lents	2	3	6	Service Compta	PREVENTIVE : Prévoir les remplacements les plus urgent si le budget le permet
	Crash Disque	3	4	12	Ancien service Info	PREVENTIVE : Prévoir des tolérances à la panne
	Windows pirate	3	4	12	Ancien service Info	CURATIVE : Réinstallation des postes clients et mesures de sécurité info
	PC Serv Comm	3	3	9	Ancien service Info	PREVENTIVE : Proposer une solution de remplacement le temps de trouver la panne
Interférence Humaine Accidentelle	Maladie / AT	2	3	6	RH	PREVENTIVE : Mesures RH
	Erreur de réalisation	2	3	6	Chef service correspondnant	PREVENTIVE : Formation et aide utilisateurs
	Erreurs d'utilisation	3	3	9	Chef service correspondnant	CURATIVE : Contrôle des applications installés sur les TIC

Diagramme en radar :



Règles régissant l'utilisation des moyens informatiques mis à disposition des salariés :

Menaces pour les données de l'entreprise :

- Prendre soin du matériel mis à disposition
- Ne pas utiliser l'outil informatique à des fins personnelles
- Ne pas naviguer sur des sites à caractère personnel
- Il est interdit de voler ou de visionner des documents personnels dont vous n'êtes pas le propriétaire
- Il est interdit d'entraver la vie privée d'autrui

Menaces et atteintes à l'image de l'entreprise :

- Il n'est pas toléré d'insulter ou de harceler des personnes au sein de l'entreprise comme par message
- Il est interdit de regarder ou de télécharger du contenu illégal
- Ne pas dénigrer l'entreprise
- Ne pas parler au nom de l'entreprise sans son approbation

Moyens à mettre en œuvre pour la sécurité des fichiers :

- Les postes de travail doivent être verrouillés manuellement et automatiquement en programmant un verrouillage de session automatique
- Les mots de passe ne doivent pas être divulgués
- Ne pas laisser son mot de passe en évidence
- Ne pas compromettre l'intégrité du réseau
- Sécuriser l'accès aux locaux sensibles aux vols de fichiers
- Chiffrer les documents sensibles
- Ne pas ouvrir de lien ou de document suspect
- Sauvegarder régulièrement ses données sur le réseau

Informations à communiquer aux salariés d'une entreprise quant à l'utilisation des outils informatiques

- Prendre soin des outils mis à disposition par l'entreprise et les utiliser à des fins professionnelles
- La messagerie et l'Internet peuvent être soumis à des contrôles et donc être limités pour :
    - Assurer la sécurité du réseau et éviter les attaques
    - Assurer un contrôle de l'utilisation trop personnel des outils informatiques mis à disposition
- Les messages reçus ou envoyés par les salariés ne sont pas copiés automatiquement par l'employeur
- Il est illégal pour l'employeur d'utiliser un « Keyloggers » qui permet d'enregistrer à distance les actions effectuées sur un ordinateur
- L'historique des événements du processus ne doivent pas être conservés plus de 6 mois
- Les fichiers des utilisateurs sont professionnels et peuvent alors être consultés par l'employeur. Pour accéder aux fichiers désignés comme personnels, l'employeur doit :
    - Être en présence du salarié ou avoir obtenu son accord
    - Être en cas d'extrême nécessité, de risque ou d'évènement particulier, juridiquement approuvé
- Les identifiants et mots de passe sont confidentiels et ne doivent être divulgués à personne. En l'absence de l'employé, si des informations indispensables à la poursuite des activités sont contenues sur son poste de travail, l'employeur peut alors exiger que ses codes soient transmis lorsque l'administrateur ne peut pas en fournir l'accès.

Disposition légale par rapport à la mise en place d'une solution de filtrage de contenu en entreprise :

- L'article 6 de la loi pour la confiance dans l'économie numérique (LCEN) mentionne l'obligation de mettre des filtres et conserver les données de connexion pendant 1 an.
- Selon l'article L34 du Code des postes et des communications électroniques (CPCE), complété par la loi relative à la lutte contre le terrorisme (2006), « *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* »

Responsabilité pénale :

- Art 121-1 du Code pénal : « Nul n'est responsable que de son propre fait »
- Art 121-2 du Code pénal : « Les personnes morales, à l'exclusion de l'État, sont responsables pénalement […] des infractions commises, pour leur compte par les organes dirigeants ou représentants »

Responsabilité civile :

- Art 1241 du Code civil (ex-article 1383) : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence »
- Les accès à certains sites sont verrouillés Car ils peuvent altérer l'image de l'entreprise. En particulier :
  - **Des sites ayant du contenu qui dépasse les limites de la liberté d'expression :** racisme, négationnisme
  - **Des sites proposant des produits et services tels que :** vente en ligne de médicaments, tabac ou alcool.
  - **Des sites possédant des contenus altérant** la protection des mineurs, des droits d'auteurs ou proposant des jeux en ligne illicites.

Mesures de protection et de sauvegarde des données

Protection des données :

- Création de comptes utilisateurs avec mots de passe de sessions, afin de sécuriser les connexions aux postes de travail et donc aux données de l'entreprise.
- Création de dossiers partagés sur le réseau pour les différents services afin de permettre l'écriture des données sur un serveur. Ces dernières seront sauvegardées tous les soirs afin de permettre une récupération si ces données venaient à être corrompues ou endommagées, et protègeront les données même en cas de crash ou panne d'un ordinateur. (Par exemple S:\ Nom du Service).
- Création de répertoires personnels sur le réseau pour les utilisateurs, afin de leur permettre d'avoir accès à ces données depuis n'importe quel ordinateur de l'entreprise relié au réseau, y compris depuis un ordinateur de remplacement (configuration identique aux standards de l'entreprise) lorsque leur matériel principal est en réparation ou s'il a dû être réinstallé à la suite d'une panne ou un crash. (Par exemple : P:\ Nom de l'Utilisateur). Ces données seront également sauvegardées.
- Les utilisateurs doivent conserver leurs données sur les lecteurs réseaux P:\ et M:\ et éviter de stocker sur les machines qui échappent à la sauvegarde journalière. Les accès à ces mêmes répertoires seront gérés afin de les limiter aux ayants droits, et ainsi éviter que des documents confidentiels des Ressources Humaines puissent être consultés par un ordinateur du service non concernés.
- Les postes de travail doivent fournir un environnement de bureau Windows standard, par défaut, avec toutes les applications nécessaires au travail des employés. En cas de problème grave au niveau du fonctionnement de l'ordinateur, il suffit de réinstaller un système d'exploitation par défaut.
- L'implémentation d'une tolérance aux pannes pour pallier les défaillances possibles sur les disques de stockage est nécessaire. Un serveur de fichiers avec plusieurs disques sera mis en place afin de créer une redondance et ainsi pallier une panne matérielle sur l'un d'eux. Un système RAID 10 sera installé : une grappe de disque assura les performances (RAID 0) et une grappe assurera la redondance, ceci grâce à l'utilisation d'un NAS 6 baies. Cette méthode tolèrera la perte de deux disques.

Protection du réseau :

- Mise en place de logiciels anti-virus et de pare-feu sur les ordinateurs de l'entreprise afin de limiter au maximum les risques de piratage et de logiciels non autorisés.
- Mise en place d'un pare-feu physique sur le réseau afin de bloquer les tentatives d'intrusions depuis les réseaux extérieurs, de filtrer les connexions entrantes / sortantes et de bloquer les requêtes non autorisées.
- Protection par mots de passes (WPA2-PSK) sur les connexions sans-fils afin de prévenir des intrusions et des connexions non autorisées.
- Protection par mots de passe des équipements réseaux et cryptage de ces mots de passe. Mise en place de messages d'avertissement afin de mettre en garde contre l'utilisation frauduleuse et non autorisée de ces équipements.

Méthodes de sauvegardes :

- Création d'un système de sauvegarde afin de pouvoir restaurer des données (personnelles et partagées) corrompues ou détruites. Mise en place de sauvegardes sur une période de 6 mois, en effectuant une sauvegarde différentielle les lundi, mardi, mercredi, jeudi, en fonction des semaines paires et impaires et une sauvegarde complète tous les vendredis. Elles s'effectueront tous les soirs en dehors des heures de bureau afin de ne pas perturber les performances sur le réseau et de ne pas gêner pas le travail des utilisateurs.
- Les sauvegardes différentielles seront stockées sur deux supports distincts, la première sur un disque dur et la seconde, stockée sur un support bande, sortie du réseau et mise dans un coffre-fort anti-feu. Sauvegarde sur deux supports afin de limiter les risques de sauvegardes corrompues. Cette méthode permet de revenir à la sauvegarde de la veille en cas de soucis majeur paralysant l'entreprise (catastrophes naturelles, logiciels malveillants ou de rançon, virus, …).
- La sauvegarde complète du vendredi sera stockée sur deux autres supports (Cloud recommandé pour un des deux supports pour une reprise d'activité plus rapide). À la fin de chaque mois, la bande du dernier vendredi du mois est utilisée pour la sauvegarde du mois terminé qui restera 6 mois disponible et stockée dans un coffre-fort anti-feu. On pourra alors remonter de 6 mois dans les sauvegardes.
- Nombre de bandes nécessaires pour rotation : 19 bandes (8 pour semaines paires et impaires, 5 pour les vendredis et 6 pour le nombre de mois). Une archive sera créée tous les ans. (Support recommandé : bande). Utilisation du logiciel Acronis.
- Stockage d'une sauvegarde complète sur des sites extérieurs et protégés afin de pouvoir recouvrir les données de l'entreprise. Possibilité de mise en place de stratégies reposant sur le cloud afin de récupérer plus rapidement ces données et d'effectuer des sauvegardes de secours.
- S'il y avait besoin de sauvegarder certains postes de travail, la solution du Snapshot, sera retenue pour son accès facile et rapide aux données de restauration.

Mesures supplémentaires de protection :

- Mise en place du chiffrement des données de l'entreprise. Utilisation de BitLocker sur les postes de travail, et mise en place de stratégies de sécurité sur les serveurs de données. Si le cloud est retenu comme solution, il faudra alors chiffrer les données avant de les envoyer hors du réseau.
- Mise en place d'onduleurs sur les appareils du réseau afin de limiter les risques liés à une coupure brutale de courant qui pourrait se révéler catastrophique pour les données de l'entreprise.

Politique de sécurité des mots de passe

- Nouvelle politique de sécurité pour les mots de passe : changer de mot de passe tous les 90 jours avec un minimum de 8 caractères, lettres, chiffres et caractères spéciaux, et l'impossibilité de réutiliser les 6 derniers mots de passe.
- Mise en place de logiciel dits « coffre-fort numérique » pour les mots de passe et ainsi éviter l'apparition de notes/post-it avec les mots de passe inscrits dessus (rappel RGPD).
- Mise en place de fiches d'aides utilisateurs consultables depuis le réseau afin d'aider les utilisateurs à la création de mots de passes forts et leur donner des moyens efficaces pour les retenir.
- Mise en place de temporisations en cas de mauvaises entrées de mots de passes répétées afin de prévenir les tentatives d'intrusions opportunistes sur les postes de travail de l'entreprise.
- Proposition, selon le budget, des solutions utilisant des cartes à puce ou la biométrie (éventuellement lors du renouvellement du parc informatique) pour les identifications et mots de passe de session si le client en fait ressentir la nécessité.

Sensibilisation du personnel

- Prendre en compte la résistance au changement des utilisateurs et prévoir des formations par un intervenant qui les accompagnera pour la transition avec les nouvelles règles de sécurité, et des rappels sur les règles d'utilisation des mots de passe.
- Edition de la nouvelle charte informatique détaillant les mesures de sécurité, les sanctions en cas de non-respect, et le code de bon comportement avec le matériel informatique de l'entreprise, qui devra être signé par tous les utilisateurs.
- Explications sur l'absolue nécessité de créer des mots de passe forts afin de protéger les données de l'entreprise et du personnel. Rappeler au personnel qu'il est un acteur important et décisif dans le processus de protection des données. Expliquer les différentes manières utilisées par les pirates afin de voler les informations de connexion des utilisateurs.
- Notes de services pour expliquer les bons comportements en matière de sécurité numérique.
- Tenir informés les utilisateurs des menaces importantes mêmes des nouvelles, afin de les sensibiliser (nouveaux ransomware, nouveau virus ravageur, …).
- Mise en place d'un affichage d'information défilant sur l'écran de veille et des écrans présent dans les salles de pauses afin de rappeler les actualités de l'entreprise et quelques rappels utiles sur la sécurité au travail, la sécurité informatique, …
- Mise en place de fiches d'aide et d'assistance / FAQ accessibles aux utilisateurs afin de les former et les sensibiliser à l'utilisation du matériel informatique.

Bilan de ce projet

Points bénéfiques :

Le point principal a été le travail en équipe. Ce projet nous a permis d'apprendre les codes de conduite et les bons comportements à avoir au sein d'une équipe qui travaille en mode projet et qui doit respecter des délais afin de fournir des livrables.

Nous avons appris à mettre en commun nos compétences propres, les mettre au service d'un projet et naturellement laisser nos compétences s'orienter vers les tâches que l'on pouvait accomplir pour permettre au projet d'avancer.

Ce projet nous a donné envie de poursuivre le chemin d'apprentissage que nous avons choisi et également l'envie d'aller encore plus loin dans les techniques et compétences liées à notre domaine d'activités.

Diffcultées et problèmes rencontrés :

Le fait de ne pas avoir désigné de chef de projet a posé quelques problèmes d'organisation au début, surtout au niveau de la planification et de la mise en place de délais pour fournir les livrables. Cependant la cohésion du groupe et notre travail d'équipe a permis de faire contre-poids et de fournir les livrables en temps voulus. Par la suite la planification de réunions a été faite et le travail s'en est retrouvé amélioré.

La partie recherches qu'il a fallu mener afin de répondre aux exigences techniques de ce projet a été très chronophage. Une meilleure utilisation des outils à notre disposition et les formations reçues durant la préparation du projet ont grandement aidé à l'amélioration de notre efficacité au travail.

Nous avons aussi pu constater les difficultés du métier de technicien système et réseau, les devoirs et obligations en matière de prestations mais aussi de fournir un service de qualité au client. Ces épreuves nous ont appris à mieux comprendre les enjeux derrière notre métier.

ANNEXES

Guide de bonne conduite dans le cadre de notre entreprise

Toute l'équipe vous souhaite la bienvenue dans notre entreprise.

Ce dépliant vous informera des exigences de System Net Corp. Nous vous invitons à le lire attentivement afin de bien comprendre notre éthique.

System Net Corp

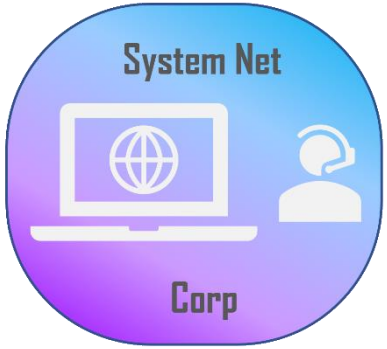
135 rue de Nancy
54390 Frouard

Contact :

Téléphone : 03 83 24 38 39
Email : contact-us@snc.net

System Net Corp

À l'attention des techniciens et du service hotline



Téléphone : 03 83 24 38 39

Respecter l'horaire du rendez-vous fixé avec le client

Soigner sa présentation, elle est le reflet de notre entreprise.

Rester professionnel et respectueux auprès des clients

Savoir s’organiser pour gérer au mieux les urgences et les demandes de la clientèle

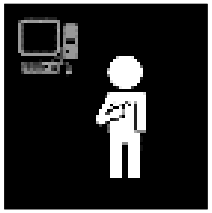
Informer le client des modifications réalisées sur son matériel

Ne pas consulter les documents confidentiels des clients

Ne pas divulguer les informations sensibles de la clientèle

Vérifier avec le client si le problème pour lequel il a appelé est résolu

Rendre au client le matériel qu'il nous a confié pour effectuer des réparations



Donner au client une estimation du temps de réparation de son matériel

Installer des versions logicielles officielles pour les clients

Être à l’écoute de son interlocuteur

Faire régulièrement des feed-back au client pour vérifier l'exactitude de ses demandes

Prévoir une solution de secours pour permettre au client de continuer son activité professionnelle

Utiliser un langage accessible à tous

Prévenir le client en cas de retard

Être poli avec tout interlocuteur

Notre charte qualité

Un conseiller commercial qui vous suit depuis le début et qui vous apporte des conseils sur mesure afin de répondre à vos besoins

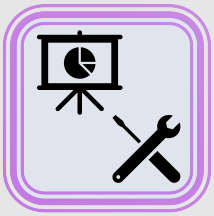
Nous intervenons sur site en moins de 2 heures, et rétablissons votre système dans les 6 heures. Nous proposons un support téléphonique 24/24 et un service d'astreinte pour vous aider

Un centre de services en plusieurs niveaux permettra de répondre à toutes les demandes et réagir face à toutes les pannes. Il saura vous guider vers la reprise d'activité après un

Notre personnel se tient à jour sur les nouvelles technologies et se forme à tous les niveaux de compétences (CCNA & ITIL). Ils sauront aussi former votre personnel et l'accompagner

Nous protégeons vos données grâce à nos différentes solutions de sauvegarde qui vous garantissent la reprise d'activité. Nous vous garantissons une confidentialité de vos données à tous niveaux

Nous tenons compte de votre équipement existant, veillons sur votre système d'information et le faisons évoluer afin de maintenir ses performances



Votre satisfaction est notre engagement car elle est le reflet de notre qualité de service. Des enquêtes par le biais d'indicateurs sont régulièrement menées afin de s'en assurer

System Net Corp – 135 rue de Nancy – 54390 Frouard

Charte Informatique

L'entreprise AutoConcept met à disposition de ses utilisateurs un système d'information et des moyens qui sont nécessaires à l'exécution de ses missions et activités qui comprend :

- Un réseau informatique
- Un réseau téléphonique

Pour pouvoir travailler, les employés sont dans l'obligation d'utiliser les ressources informatiques mises à leur disposition par l'entreprise. L'utilisation du système d'information et de communication se fait exclusivement à des fins professionnelles, sauf exception prévue dans la présente charte. Pour une question de transparence, cette charte informatique a pour but de faire connaître les règles d'usages de ces ressources. Les moyens de contrôle et de surveillance mis en place sont également définis pour la bonne exécution du contrat de travail des salariés mais aussi dans le cadre de la responsabilité pénale et civile de l'employeur. Les lois en vigueur que nul n'est censé ignorer ne sont en aucun cas remplacés par cette présente charte.

Table des matières

Article I : A qui s'applique-t-elle ?

La charte ici présente, concerne tous les utilisateurs utilisant le système d'information, notamment :

- Les salariés
- Les intérimaires
- Les visiteurs
- Les dirigeants
- Les employés de sociétés prestaires
- Les stagiaires
- Les intervenants externes

Article II : Contenu du parc informatique.

Le parc informatique est composé :

- d'ordinateurs
- d'imprimantes
- de serveurs
- de routeurs
- de périphériques
- de smartphones
- de tablettes

Pour assurer la sécurité du système d'information (parc informatique + logiciels), la charte ici présente vaut pour tout matériel connecté au système d'information de l'entreprise, y compris le matériel personnel des utilisateurs noté dans l'article I.

Article III : Règles d'utilisation

Tout matériel fourni par l'entreprise doit être utilisé à des fins professionnelles, en toute conformité avec les objectifs de l'organisation, sauf cas exceptionnel, ou accepté par la loi.

Le système d'information de l'organisation ne doit en aucun cas être utilisé pour mener des activité concurrentes et/ou susceptibles de porter atteinte à l'organisation de quelque manière que ce soit.

Article IV : Sécurité informatique

IV. 1 Rôle de l'entreprise :

L'entreprise va mettre en œuvre des moyens pour sécuriser les informations, personnelles ou professionnelles de ses employés et peut donc limiter certains accès à des ressources.

La direction informatique est responsable de la mise en œuvre et du contrôle du bon fonctionnement du système d'information. Un plan de sécurisation et un plan de continuité des services, en particulier lors de défauts de matériel doivent être établis. La direction doit veiller à faire respecter cette charte et de mettre ces règles en vigueur.

IV. 2 Responsabilité de l'utilisateur :

Les ressources confiées à l'utilisateur dans le cadre de l'exercice de ses fonctions sont sous sa responsabilité. Il est de son devoir de concourir à la sécurité de ses ressources, en faisant preuve de vigilance et de prudence. L'utilisateur doit utiliser ses ressources uniquement dans le cadre de sa mission. S'il est témoin d'une tentative ou d'une violation de l'intégrité des ressources, de tout dysfonctionnement, incident ou anomalie, il doit impérativement le signaler à l'équipe informatique. Sauf si autorisation de la part de la direction informatique, il est interdit d'accéder au système d'information avec du matériel extérieur (Ordinateurs portables, périphériques tel que la clé USB).

Si l'utilisateur est autorisé à utiliser du matériel extérieur, il est de son devoir de veiller à la sécurité du matériel utilisé. La sortie de matériel doit être autorisée par la direction et uniquement pour un usage professionnel.

Même temporairement, si un utilisateur doit s'absenter de son poste de travail, il ne doit pas oublier de verrouiller sa session.

L'utilisateur doit régulièrement faire des sauvegardes de ses données sur les zones de stockages en réseau mis à disposition, cela permet d'éviter toute perte de données due à un problème matériel. L'utilisateur doit supprimer toute donnée inutile des zones de stockage pour ne pas les surcharger. Si des données anciennes doivent être sauvegardées, un archivage des données sera effectué.

L'utilisateur a l'interdiction d'installer ou supprimer des logiciels, de copier des fichiers susceptibles de créer des risques de sécurité au sein de l'entreprise. La modification des paramétrages du poste de travail ou des outils mis à disposition est interdite. Il ne doit pas non plus contourner les systèmes de sécurité mis en œuvre dans l'entreprise. Pour toute modification, l'utilisateur doit contacter le service informatique.

L'utilisateur est dans l'obligation de se conformer à la législation, protégeant les droits de propriétés intellectuelles, les données personnelles, le secret des correspondances, le système de traitement automatisé de données, le droit à l'image, l'exposition des mineurs à du contenu préjudiciable. Il ne doit en aucun cas se livrer à une activité concurrente à celle de son entreprise ou susceptible de lui porter préjudice en utilisant son matériel professionnel.

IV. 3 Obligation générale de confidentialité

L'utilisateur s'engage à préserver la confidentialité des informations, en particulier des informations personnelles, traitées sur le système d'information de l'entreprise.

Il doit donc s'engager à ne pas divulguer lui ou une personne sous sa responsabilité, des informations confidentielles.

IV. 4 Mot de passe

L'accès au système d'information est protégé par des mots de passe individuels. Il doit être strictement confidentiel afin de permettre à chacun d'avoir ses propres autorisations et de garder pour eux leurs dossiers confidentiels. Le mot de passe ne doit pas être écrit sur une note visible de tous, il est à retenir. Il ne doit pas non plus être donné à quelqu'un ou accessible par d'autres personnes. Lors de chaque accès au système d'information, l'identifiant et le mot de passe doivent être demandés.

Le mot de passe doit être conforme à la politique de mot de passe prescrit par la CNIL relative à la protection des données personnelles, notamment :

- Composé de 8 caractères ;
- Ces caractères doivent être une combinaison de chiffres et de lettres ;
- Il doit posséder des majuscules et des minuscules
- Il est idéalement conseillé d'y insérer des caractères spéciaux

Article V : Accès à Internet

V. 1 Accès aux sites

Dans le cadre de leurs travaux, les utilisateurs pourront avoir accès à l'Internet. Pour des raisons de sécurité et de déontologie, l'accès à certains sites sera restreint ou prohibé par le service informatique qui est habilité à imposer des configurations de navigateur et à installer des mécanismes de filtrage.

L'utilisation d'Internet se fait uniquement dans le cas de l'activité professionnelle. Il est alors strictement interdit d'utiliser Internet à des fins personnelles pouvant permettre un gain financier ou le soutien d'activités lucratives. Il est également interdit de créer ou mettre à jour tout site internet via l'infrastructure de l'entreprise.

Il est défendu d'utiliser l'Internet pour aller sur des sites dont le contenu est contraire à l'ordre public, ou à l'image de l'entreprise, ainsi qu'aux sites pouvant impacter la sécurité du système d'information de l'entreprise ou engageant financièrement celle-ci

V. 2 Autres utilisations

L'utilisation d'Internet visant à discuter sur des forums de discussion, chats en ligne, système de discussion instantanée est autorisée uniquement à des fins professionnelles et sur autorisation de la direction ayant pris contact avec le service informatique.

Il est interdit de procéder à un téléchargement de fichiers, en particulier les fichiers multimédias, sauf en cas de justification professionnelle validée par la hiérarchie.

Pour rappel, les utilisateurs ne doivent pas se livrer à des activités illicites ou portant atteinte aux intérêts de la société sur Internet.

Pour information, des enregistrements sont faits pour garder des traces des sites visités par les utilisateurs. Ceux-ci pourront être exploités à des fins statistiques et de contrôles dans les limites prévues par la loi, en particulier lors d'une forte perte de bande passante sur le réseau de l'entreprise.

Article VI : Messagerie électronique

Pour l'exercice de ses missions, tout employé peut disposer d'une adresse de messagerie électronique.

Dans la logique, chaque courriel envoyé l'est à titre professionnel.

Exceptionnellement, les employés peuvent utiliser leurs adresses de messagerie électroniques à des fins personnelles dans les limites posées par la loi. Les messages personnels porteront alors la mention "PRIVE" et devront être rangés dans un répertoire appelé "PRIVE" dans la messagerie.

Article VII : Sanctions

Si les règles précédemment énoncées ne sont pas respectées, il est dans le droit de l'entreprise d'engager des poursuites judiciaires à l'encontre de l'utilisateur n'ayant pas respecté la charte.

Article VIII : Adhésion de la charte

En acceptant cette charte ici présente dictant les bons usages du système d'information et de communication de l'entreprise, cela implique l'acceptation sans réserve de toutes les conditions générales d'utilisation des services numériques et des chartes d'usage qui leurs sont associées. L'utilisation du service informatique entraine obligatoirement l'acceptation de sa propre charte sans réserve de la part de l'utilisateur.

Article IX : Entrée en vigueur

La charte si présente est ajoutée dans l'annexe du règlement intérieur et communiqué à chaque employé.

Elle entre en vigueur au 3 décembre 2019

Je soussigné(e) ..... , atteste avoir pris connaissance de la « Charte informatique » de l'entreprise System Net Corp et m'engage à la respecter.

Fait à ..... , le .....