T3ckCorp
21 rue Alix Le Clerc, 54700 NANCY
Numéro Tel : 03 89 75 25 61

T3ckCorp

Maxime GUERESCHI - Jean-Gabriel DRON - Timothée FOUREL

Table des matières :

Nom de l'entreprise : T3ckCorp

Logo entreprise :

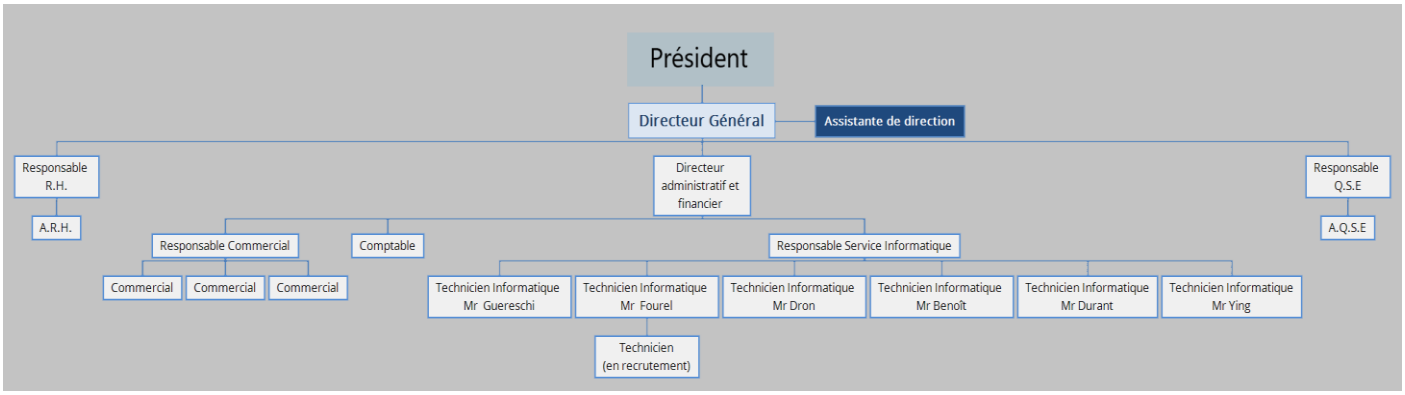
Situation géographique :

21 rue Alix Le Clerc
54000 NANCY

Coordonnée GPS :
-Latitude 48.701663
-Longitude 6.165000

Téléphone : 03 89 75 25 61
Courriel : contact@t3ckcorp.com

Organigramme :



Outils utilisés :

L'internet : 

Xmind : 

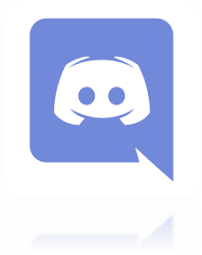
Slack : 

PDF : 

Word : 

PhotoFiltre : 

Excel : 

Discord : 

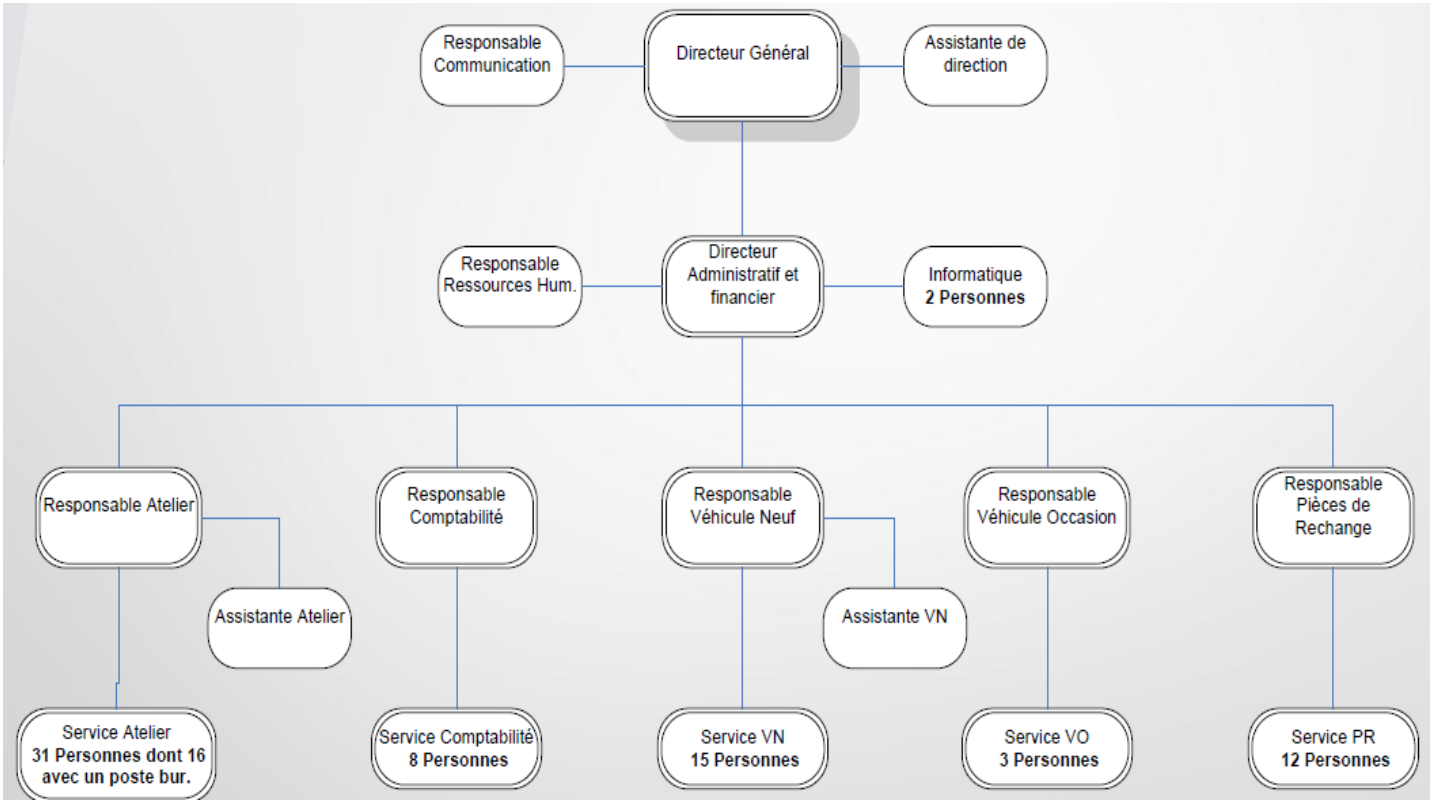
PowerPoint : 

Étude de l'existant :

AutoConcept

L'entreprise AutoConcept est un concessionnaire automobile. Cette dernière est constitué d'environ 80 employés, comprenant un parc informatique de 70 à 80 postes, et souhaitant externaliser les prestations informatiques qui sont actuellement exécutées par deux informaticiens en internes.

Organigramme



Problématique :

-Parc informatique en perte de vitesse et de vitalité :

Le parc informatique d'AutoConcept est sujet à plusieurs types de problèmes, tels que :

-des lenteurs sur certains postes
-des crashs de disques dur
-des messages intempestifs de <<version Windows pirates>> sur certains postes d'utilisateurs

Un crash de disque dur d'une commerciale est déjà survenu avec une perte d'exploitation de 80000 euros pour l'entreprise AutoConcept.

Ces problèmes empêchent d'amortir correctement le matériel informatique sur 3 ans comme l'avait choisi l'entreprise AutoConcept, sans oublie que la chef comptable est très réticente à tout renouvellement avant la fin de la période d'amortissement.

Pour assurer la survie et le bon fonctionnement du parc informatique d'AutoConcept, il est vital pour ce dernier, d'avoir à sa disposition des techniciens qualifiés qui pourront assurer la pérennité du parc informatique

-Manque de professionnalisme de la part des techniciens :règles

Plusieurs plaintes ont été faite par des utilisateurs vis-à-vis des techniciens du service informatique d'AutoConcept.

Les points qui reviennent le plus sont les suivants :

-Les délais d'intervention du SAV sont bien trop important et les solutions apportées ne sont pas toujours viable, ainsi qu'un suivi qui pour la plupart du temps est incertain

-L'attitude, la tenue vestimentaire et la ponctualité des techniciens ne sont pas toujours correcte ainsi que le vocabulaire utilisé est parfois trop technique pour les utilisateurs.

-Le service informatique n'est pas assez à l'écoute des utilisateurs, cela conduit à des erreurs et perte de matériels.

-Les problèmes rencontré par les utilisateurs ne sont pas toujours pris en compte ou à temps par le service informatique, en plus d'un service téléphonique qui laisse à désirer.

-Un manque de communication du service informatique est à constaté vis-à-vis de ses utilisateurs.

Pour l'image d'Autocept auprès de ses utilisateurs, il est impératif de corriger les problèmes cités en amont au plus vite, surtout qu'une perte d'exploitation de 60000 euros est déjà à déplorer.

-Atteinte à la vie privée :

Certains utilisateurs de l'entreprise AutoConcept ont signalés une potentielle atteinte de leurs vie privée, les problèmes rencontrés sont les suivant :

-Intrusion d'un client sur un poste d'une commerciale dépourvue de mot de passe.

-Un utilisateur soupçonne le SAV d'avoir consulté des documents sur son poste lors d'une intervention, de plus ces informations ont été divulguées à des tiers.

Il serait préférable, pour l'entreprise Autoconcept, d'instaurer une charte informatique, ainsi qu'une politique de sécurité basé sur l'adoption de mots de passe, afin d'éviter à l'avenir, tous problème d'atteinte à la vie privée.

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

Le contrôle de l'utilisation de la messagerie électronique professionnelle :

Droit de la direction et de l'employeur :

La direction ou l'employeur a le droit d'interdire une correspondance privée même si cette dernière est protégée par « le secret des correspondances ».

La direction ou l'employeur peut mettre en œuvre des outils de contrôles mais doit respecter l'article 8 de la convention européenne des droits de l'homme selon lequel » le salarié a droit, même au temps et lieu de travail, au respect de l'intimité de sa vie privée ».

La direction ou l'employeur a le droit de contrôler la messagerie professionnelle de ses salariés en respectant les règles de la jurisprudence.

La direction ou l'employeur ne peut consulter les mails privés de ses salariés d'après l'arrêt de la cour de cassation de 2001, sauf cas particuliers qui doivent respecter certaines conditions :

-le salarié doit être présent ou prévenu

-il doit y avoir risque ou événement majeur

Il est recommandé pour la direction d'informer ses salariés, qu'il existe des procédures de contrôle et d'archivage ainsi que la durée de conservation sur la messagerie électronique. Cette information peut être communiquée par voie d'affichage et les utilisateurs doivent être informés par les administrateurs du réseau.

En cas d'absence d'un employé, ce dernier doit communiquer à son employeur les documents nécessaires à la poursuite de l'activité de l'établissement. Toutefois,

l'employeur doit préalablement définir en concertation et diffusées auprès de l'ensemble des employés susceptibles d'être concernés (via une charte par exemple).

Pour la mise en place de tous dispositif de filtrage informatique de données personnelles dans une entreprise, il est obligatoire pour l'entreprise en question de le communiquer à la CNIL

Droit du salarié :

Le salarié a le droit de classer systématiquement ses messages dans un dossier personnel, et de l'éditer comme étant un message « personnel ».

Le contrôle de l'utilisation de l'internet :

L'entreprise peut interdire l'utilisation d'internet à des fins privés, même si cela n'est pas recommandé dans une société d'information et de communication. Un usage raisonnable serait plus recommandé, si cela ne met toutefois pas en cause la productivité générale des salariés.

L'entreprise peut rédiger une charte d'utilisation d'internet. Celle-ci peut prévoir :

- Des dispositifs de filtrages (sites à caractères pornographiques, de pédophilie, d'incitation à la haine raciale, etc.)
- L'interdiction de télécharger des logiciels, de se connecter à des forums, d'utiliser le « chat » ou de se connecter à sa boite mail personnel pour éviter tout risque de virus.

L'entreprise doit en informer ses utilisateurs si cette dernière décide d'instaurer des dispositifs de filtrages.

Si l'entreprise décide de mettre en place un dispositif de contrôle individuel de ses employés destinés à produire, poste par poste, un relevé des durées de connexion ou des sites visités, le traitement automatisé de données à caractère personnel ainsi mis en œuvre doit être déclaré au CNIL.

La durée de conservation des données devra être indiquée par l'entreprise. Une durée de conservation de l'ordre de six mois devrait être suffisante.

Contenu général d'une charte informatique (Clauses-Validation-diffusion) :

Clauses :

Il conviendra, en tout état de cause, de rédiger un préambule permettant, en cas de contentieux, de déterminer l'interprétation qui devra être donnée à un certain nombre de clauses.

Par ailleurs, il est indispensable de fixer les conditions de confidentialité liées à l'utilisation de certains outils informatiques.

L'accès à Internet doit également faire l'objet de dispositions particulières. Il pourra être rappelé les risques d'infractions encourues par le salarié pendant les heures de travail (téléchargements, etc.).

Par ailleurs, il conviendra aussi de rappeler la responsabilité pénale et civile encourue par l'employeur au titre des agissements de ses salariés sur Internet pour mieux encadrer, d'une part, certaines exonérations de responsabilité et permettre, d'autre part, la justification éventuelle de certaines mesures de cybersurveillance. Il convient de noter qu'en tout état de cause, l'employeur ne peut interdire en totalité l'accès à Internet sur le lieu de travail.

Concernant la messagerie électronique, il conviendra de traiter à la fois l'utilisation de la messagerie personnelle, de la messagerie professionnelle et de la messagerie instantanée ou "chat".

Il devra également comprendre des dispositions relatives aux moyens de contrôle utilisés et aux pouvoirs des Administrateurs systèmes (enquête, etc.). En effet, à défaut d'informer les salariés sur les dispositifs de contrôle existants, l'employeur ne peut se prévaloir des preuves relevées par lesdits dispositifs.

Enfin, il paraît particulièrement intéressant de prévoir la mise en place d'une convention de preuve.

En tout état de cause, la charte informatique, tout comme le règlement intérieur, ne doivent pas contenir de « dispositions apportant aux droits des personnes et aux libertés individuelles et collectives des restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché », ce principe conducteur étant valable pour toutes les clauses de ladite charte et notamment celles énoncées ci-dessus

Validation :

Ainsi, en cas de mise en place de dispositifs de contrôle informatique, il conviendra d'accomplir les formalités auprès de la CNIL et relatives à la mise en place de procédés de cybersurveillance. En effet, une déclaration (normale ou simplifiée) ou une autorisation pourra éventuellement s'avérer nécessaire.

Diffusion :

Une fois rédigée et validée (selon le contenu retenu et l'organisation propre à chaque organisme : par la DRH, la Direction juridique, avec ou sans consultation des représentants du personnel, a priori sans consultation préalable de l'Inspection du Travail), la charte doit être communiquée largement au sein de l'organisme.

Une action ponctuelle de communication doit être prévue mais on veillera à ce que le contenu de la charte soit à l'esprit de chaque acteur dans la continuité.

Voici quelques exemples d'action ponctuelle de communication pour la charte « salarié » pouvant être retenues (combinaisons possibles) :

a. Diffusion du support papier avec le bulletin de salaire, accompagné d'une lettre d'accompagnement du dirigeant («je compte sur vous »)

b. Diffusion du support dans le journal interne ou sur une note « Actualités » (support papier et/ou intranet)

c. Création d'un *leaflet* adressé aux managers accompagnés d'un mot du dirigeant, les invitant à commenter le support à leurs équipes.

Charte informatique (en annexe) :

(Voir document en annexe)

Formalités particulières – Déclarations :

La mise en place d'une charte informatique est soumise à certaines formalités, en cas de choix du règlement intérieur comme support et concernant les IRP, l'inspection du travail et le dépôt au greffe du conseil de prud'hommes. Néanmoins, la mise en place d'une charte informatique peut s'accompagner de formalités adjacentes et dépendant du contenu même de la charte.

Ainsi, en cas de mise en place de dispositifs de contrôle informatique, il conviendra d'accomplir les formalités auprès de la CNIL et relatives à la mise en place de procédés de cybersurveillance. En effet, une déclaration (normale ou simplifiée) ou une autorisation pourra éventuellement s'avérer nécessaire.

Moyens à mettre en œuvre pour la sécurité des fichiers :

Avant de mettre en œuvre un moyen de sécurisation des fichiers, il faut tout d'abord définir les différents objectifs qui sont :

-La disponibilité : le système doit fonctionner sans faille durant les plages d'utilisation prévues et garantir l'accès aux services et ressources installées avec le temps de réponse attendu.
-L'intégrité : les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets.
-La confidentialité : seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées. Tout accès indésirable doit être empêché.

D'autres aspects peuvent aussi être considérés comme des objectifs de la sécurité des systèmes d'information, tels que :

-La traçabilité : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.
-L'authentification: l'identification des utilisateurs est fondamentale pour gérer les accès aux espaces de travail pertinents et maintenir la confiance dans les relations d'échange.
-La non-répudiation et l'imputation : aucun utilisateur ne doit pouvoir contester les opérations qu'il a réalisées dans le cadre de ses actions autorisées et aucun tiers ne doit pouvoir s'attribuer les actions d'un autre utilisateur.

Une fois les objectifs de la sécurisation déterminés, les risques pesant sur chacun de ces éléments peuvent être estimés en fonction des menaces. Le niveau global de sécurité des systèmes d'information est défini par le niveau de sécurité du maillon le plus faible. Les précautions et contre-mesures doivent être envisagées en fonction des vulnérabilités propres au contexte auquel le système d'information est censé apporter service et appui.

Il faut pour cela estimer :

-La gravité des conséquences au cas où les risques se réaliseraient ;

-La vraisemblance des risques (ou leur *potentialité*, ou encore leur *probabilité d'occurrence*).

Ensuite il faut effectuer les démarches générales pour sécuriser le système d'information qui sont évaluer les risques et leurs criticités, rechercher et sélectionner les parades, mettre en œuvre les protections et vérifier leurs efficacités

Quelques exemples de moyens à mettre en œuvres pour la sécurité des fichiers :

- ✔ Adopter une politique de mot de passe rigoureuse
- ✔ Concevoir une procédure de création et de suppression des comptes utilisateurs
- ✔ Sécuriser les postes de travail
- ✔ Identifier précisément qui peut avoir accès aux fichiers
- ✔ Veiller à la confidentialité des données vis-à-vis des prestataires
- ✔ Sécuriser le réseau local
- ✔ Sécuriser l'accès physique aux locaux
- ✔ Anticiper le risque de perte ou de divulgation des données
- ✔ Anticiper et formaliser une politique de sécurité du système d'information
- ✔ Sensibiliser les utilisateurs aux « risques informatiques » et à la loi "informatique et libertés"

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

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité. Chaque employé doit être notamment informé :

→ Des finalités poursuivies,

→ De la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),

→ Des destinataires des données,

→ De la durée de conservation des données,

→ De son droit d'opposition pour motif légitime,

→ De ses droits d'accès et de rectification,

→ De la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service.

-Quelles formalités :

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre des dispositifs de contrôle.

Les différents systèmes de contrôle des outils informatiques doivent être inscrits au registre des activités de traitement tenu par l'employeur.

-Quels recours :

En cas de difficultés, vous pouvez vous adressez aux :

-les services de l'inspection du Travail
-le procureur de la République
-le service des plaintes de la CNIL, sur les modalités de mise en œuvre d'un dispositif de contrôle de l'activité.

Textes de références :

- Le code civil : Article 9 (protection de l'intimité de la vie privée)
- Le code du travail : Article L. 1121-1 (droits et libertés dans l'entreprise)
  Article L. 1222-3 et L. 1222-4 (information des employés)
  Article L. 2323-47 (information/consultation du comité d'entreprise)
- Le code pénal : Articles 226-1 et suivants (protection de la vie privée)
- Le Règlement européen sur la protection des données personnelles (RGPD)

Dispositions légales relatives à la mise en place d'une solution de filtrage de contenu en entreprise :

L'employeur doit veiller à ce que les modalités d'utilisation de la solution respectent les dispositions réglementaires.

-Les catégories de filtrages doivent être non discriminatoire :

S'il est normal, voire obligatoire d'interdire l'accès à certains contenus (pédopornographie, racisme, téléchargement illégal…) certaines restrictions constituent une discrimination.

Ainsi, créer une politique de filtrage autour de thématiques telles que l'homosexualité peut être considéré comme une atteinte aux libertés fondamentales des individus. De même, l'outil de filtrage ne doit pas disposer de catégorie de ce type, permettant aux administrateurs d'avoir accès à des informations, telles que l'orientation sexuelle, qui relèvent de la vie privée.

-Le blocage doit être non discriminatoire :

Prenons l'exemple de la politique, les administrateurs de la solution ne peuvent pas autoriser les sites d'un certain bord politique et bloquer les autres en fonction de leurs convictions personnelles (même chose avec les religions).

-Les politiques de filtrages doivent être les mêmes d'un salarié à un autre occupant le même poste :

Il est essentiel d'assurer le même niveau de paramétrage de la solution pour tous les utilisateurs occupant un même poste, afin de ne pas discriminer les utilisateurs.

Cependant, si un utilisateur met en péril la sécurité du système d'information, il peut être justifié de limiter ses accès Internet. Il convient d'avoir préalablement informé l'employé de cette possibilité (par exemple en prévoyant un paragraphe spécifique sur ce type de sanction dans la charte Internet), et de l'informer individuellement par mail ou par courrier que son accès va être limité.

-Déclaration à la CNIL :

Un outil de filtrage permet l'accès à des données à ″caractère personnel″. Ces données peuvent être collectées, saisies, enregistrées, éditée. Elles font donc l'objet d'un traitement. De ce fait, toute personnes qui met en œuvre un outil de filtrage permettant un contrôle individuel, doit obligatoirement déclarer cet outil à la CNIL (sauf si l'entreprise dispose d'un CIL)

Déclaration dite NORMALE de la CNIL :

-déclaration normale de la CNIL

-la finalité du traitement

-les données à caractère personnel traitées

-la finalité du traitement

-les catégories de personnes concernées

-la durée de conservation des données

-l'indication de la date à laquelle les instances représentatives du personnel ont été consultées sur la mise en place des outils de filtrage

Politique de sécurité basée sur l'adoption du mot de passe

Choix du mot de passe :
Celui-ci ne doit pas être trop simple et vous ne devez pas utiliser les dates de naissance de vos proches ou encore vos passe-temps car ils seront trop faibles pour quelqu'un de mal intentionné, de plus il faudra utiliser des caractères numériques telle que / - * _ … et aussi un chiffre.

C'est donc pour c'est raison que votre mot de passe devra contenir 10 caractères avec :

- 1 chiffre
- Un caractère alphanumérique
- Une Majuscule
- Une minuscule

Exemple : Kia_Ppbr/9

En plus de tous cela il y a quelques règles à respecter :

- Ne pas écrire sur papier son mot de passe
- Ne pas partager un compte utilisateur
- Ne pas utiliser le même mot de passe pour différents accès
- Ne jamais communiquer son mot de passe
- Ne jamais donner son mot de passe, même aux personnes chargées de la sécurité
- Se déconnecter avant de quitter son poste
- Changer le mot de passe au moindre soupçon de compromission

Sensibilisation des utilisateurs a la nécessité d'adopter cette politique de sécurité :

Étant donné que tout le monde n'est pas bien intentionné sur cette planète et que c'est d'autant plus valable dans le domaine informatique, il faut se protéger, comment peut-on faire :

On peut mettre des mots de passe pour protéger ses comptes, c'est une clé numérique qui nous permet d'ouvrir la porte derrière laquelle on stock nos donnée, comme lorsque vous fermez à clé avant de partir de chez vous pour protéger vos bien, ou en l'occurrence ceux de l'entreprise, les données de l'entreprise ont une grande valeur et sans celle-ci elle ne peut pas fonctionner, aussi vous devez de manière individuelle protéger votre accès à c'est donné, en commencent par verrouiller son ordinateur par un mots de passe.

Voir : Politique de sécurité basée sur l'adoption du mot de passe

Vous êtes aussi conviées à une journée de formation et d'information sur la sécurité informatique, qui sera présenté par un de nos expert et vous trouverez dans votre boite mail et sur les divers écrans d'informations de votre entreprise :

- Des contenus essentiels et tenus à jours
- Des cours personnalisés répartis sur diverses thématiques liées à la cybersécurité
- Des cours interactifs et stimulant, de quelques minutes à plusieurs heures selon les besoins
- Une plateforme d'administration ludique et ergonomique
- Des infos pour suivre des indicateurs clés

Mesures de protection et de sauvegarde des données :

Pour la partie protection des données, nous mettrons en place un antivirus sur chaque machine, celui retenue pour le moment est : Kaspersky, il sera géré à distance par nos services et nous vérifierons sont bon fonctionnement.

Quant à la partie de sauvegardes des données il y aura un serveur de sauvegarde qui va être mis en place dans une pièce sécuriser, avec un accès restreint au personnel qualifié qui effectuera une sauvegarde sur bande, et une copie sera envoyer et sauvegarder dans nos locaux spécialiser dans le cas où un incident (dégât des eaux, incendie …) arriverai sur vos locaux.

La sauvegarde, sera effectuer toute les Heures sur votre serveur local et une copie nous sera envoyer en fin de journée et sera donc stocker sur notre site spécialiser, en cas de pertes de vos données, la sauvegarde sera donc redéployée sur vos machines dans les plus brefs délais.
De notre coter nous assurons un taux maximal de conservation et de récupération de vos données

Nos infrastructures à la pointe de la technologie nous permettent de conserver de manière sûre et sécuriser les données stockées sur nos serveurs, qui sont redonder et qui sont eux même quotidiennement sauvegarder.

Charte Qualité :

(voir document en annexe)