IDK

LA TECHNOLOGIE A VOTRE SERVICE

Etude de cas AutoConcept

Projet SAS

CESI de PAU – GMSI 17

Marion DUBOURG – Thomas POTIN – Julien VILLARD

IDK

Table des matières

Introduction

L'entreprise AutoConcept se trouve dans une situation délicate car son système d'information ne répond pas aux besoins, présente des failles de sécurité et aucune stratégie opérationnelle ne semble mise en place.

Cela impacte directement l'économie de l'entreprise et a un impact négatif sur ses performances. A plus long terme l'impact pourrait conduire l'entreprise dans une situation de grande précarité économique.

En regardant en détail les différents problèmes remontés dans le compte-rendu du service commercial on peut noter plusieurs points :

- En premier lieu un aspect légal regroupant les problématiques d'utilisation du système d'information en entreprise.
- Dans un deuxième temps un aspect technique qui englobe le matériel, le logiciel, la sécurisation des données et la mise en place des stratégies opérationnelles.
- Dans un troisième temps un aspect humain qui englobe la sécurisation des données, l'utilisation du matériel, les bonnes pratiques professionnelles et le management.

Après avoir analysé les problématiques, nous pouvons proposer, à travers cette note de synthèse, des préconisations concernant les aspects légaux, la sécurisation des données, l'utilisation du matériel et des logiciels mais aussi concernant les aspects managériaux et de formation.

I. Partie légale

⇨ Le Droit et l'informatique

Pour comprendre le Droit de l'informatique (plus rarement appelé "droit informatique"), il est indispensable de prendre connaissance des grands textes de lois. Le Droit informatique est, dans ce sens, une matière extrêmement vaste et transversale puisqu'elle intéresse :

- Le droit civil (notamment le droit des contrats) ;
- Le droit commercial ;
- Le droit pénal (intrusions frauduleuses dans les systèmes d'informations) ;
- Les libertés publiques (loi informatique et libertés) ;
- La propriété intellectuelle (droit d'auteur sur les logiciels, brevets sur les "puces", etc.) ;
- Le droit de l'internet (Hadopi 2).

Dans le contexte actuel, AutoConcept est face à de sérieuses problématiques où sa propre responsabilité peut être mise en cause. L'absence de charte informatique, de solution de filtrage, et de sécurisation des données personnelles, sont des problèmes pouvant remettre en cause la pérennité de l'entreprise.

A. Les codes et l'autorité administrative indépendante (AAI)

Afin de comprendre la réglementation en vigueur sur l'utilisation d'outils informatiques, nous verrons l'utilité des codes de loi et l'autorité administrative indépendante compétente dans le domaine.

🕮 Commission Nationale de l'Informatique & Liberté

Article 1 Modifié par LOI n°2016-1321 du 7 octobre 2016 - art. 54

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

Toute personne dispose du droit de décider et de contrôler les usages qui sont faits des données à caractère personnel la concernant, dans les conditions fixées par la présente loi.

La **Commission nationale de l'informatique et des libertés** (la **CNIL**) de France est une autorité administrative indépendante. Cette dernière est chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques. Elle exerce ses missions conformément à la loi Informatique et Liberté nº 78-17 du 6 janvier 1978 modifiée le 7 Octobre 2016.[1]

La CNIL étant une Autorité Administrative Indépendante, présente trois caractères :

- L'autorité : elle est l'unique autorité sur l'application des articles de loi 78-17 Informatique et Liberté.
- L'administration : elle agit au nom de l'Etat, par conséquent elle dispose de certaines compétences administratives.
- L'indépendance : elle ne peut être « contrôlée » par l'état ou toute autre forme de contrôle.

[1] Voir annexe 1

Elle est investie de six missions, qu'elle se doit de remplir :

- Informer : elle informe les personnes sur leurs droits et leurs obligations
- Réguler : elle recense et régule les fichiers publics et gouvernementaux.
- Protéger : elle veille à ce que les citoyens soient informés des données collectées et traitées sur leur compte. Elle donne la permission à l'accès des données de l'Etat.
- Anticiper : elle fait une veille perpétuelle de nouveaux systèmes d'informations.
- Contrôler : elle investigue les traitements informatiques dans les locaux professionnels pour s'assurer que la loi soit respectée. Elle surveille la sécurité de tous les systèmes d'informations.
- Sanctionner : elle avertit ; applique des sanctions pécuniaires ; fait injonction de cesser toute activité de traitement. Le procureur peut être saisi par le président de la commission pour violation de la loi.

🕮 Code pénal

Article 121-2 Modifié par Loi n°2004-204 du 9 mars 2004 - art. 54 JORF 10 mars 2004 en vigueur le 31 décembre 2005

Les personnes morales, à l'exclusion de l'Etat, sont responsables pénalement, selon les distinctions des articles 121-4 à 121-7, des infractions commises, pour leur compte, par leurs organes ou représentants. (…) La responsabilité pénale des personnes morales n'exclut pas celle des personnes physiques auteurs ou complices des mêmes faits, sous réserve des dispositions du quatrième alinéa de l'article 121-3.

Tout utilisateur de moyen informatique se doit de respecter la loi, sans quoi des sanctions pénales peuvent être applicables. Le risque pénal revient à répondre des infractions et donc d'être sanctionné pénalement. Dans le contexte actuel d'AutoConcept, il est important de rappeler les risques qu'encourent les salariés ainsi que la firme.

🕮 Code de la propriété intellectuelle

Article L335-2 Modifié par LOI n°2016-731 du 3 juin 2016 - art. 44

Toute édition d'écrits, de composition musicale, de dessin, de peinture ou de toute autre production, imprimée ou gravée en entier ou en partie, au mépris des lois et règlements relatifs à la propriété des auteurs, est une contrefaçon et toute contrefaçon est un délit.

La contrefaçon en France d'ouvrages publiés en France ou à l'étranger est punie de trois ans d'emprisonnement et de 300 000 euros d'amende. (…)

Lorsque les délits prévus par le présent article ont été commis en bande organisée, les peines sont portées à sept ans d'emprisonnement et à 750 000 euros d'amende.

Les articles du code de la propriété intellectuelle veillent à sauvegarder les créations d'intelligences humaines. Ils sanctionnent toute personne usant de biens immatériels ou matériels.

🕮 Code civil

Article 1242 Modifié par Ordonnance n°2016-131 du 10 février 2016 - art. 2

On est responsable non seulement du dommage que l'on cause par son propre fait, mais encore de celui qui est causé par le fait des personnes dont on doit répondre, ou des choses que l'on a sous sa garde. (…)

Le Code civil rassemble les lois relatives au droit civil français. C'est l'ensemble des règles qui déterminent le statut de personne, celui des biens et celui des relations entre les personnes privées.

⇨ L’entreprise et ses Obligations

Afin de voir sa responsabilité écartée en cas de mauvaises intentions d’un de ses employés, une entreprise peut mettre en place des solutions de filtrages. Cependant, il existe une réglementation qui se doit de ne pas être prise à la légère, sous peine d’être sanctionnable. C’est pourquoi nous allons vous informer sur les différentes obligations tant dans la conservation de données personnelles que dans le déploiement d’outils de contrôle et de surveillance.

A. Solutions de filtrage

Article 6 Modifié par LOI n° 2013-1168 du 18 décembre 2013 - art. 20 (V) - Modifié par LOI n°2014-873 du 4 août 2014 - art. 57

I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens.

Les personnes visées à l'alinéa précédent les informent également de l'existence de moyens de sécurisation permettant de prévenir les manquements à l'obligation définie à l'article L. 336-3 du code de la propriété intellectuelle et leur proposent au moins un des moyens figurant sur la liste prévue au deuxième alinéa de l'article L. 331-26 du même code.

Le filtrage consiste à donner l’accès à des « données à caractère personnel ». Les données recueillies peuvent être saisies, archivées, exploitées, et éditées. Dans tel cas, une firme qui met en place un outil de filtrage permettant un contrôle au cas par cas, se verra dans l’obligation de le déclarer à la CNIL (sauf si l’entreprise dispose d’un Correspondant Informatique et Liberté ou CIL).

En vertu de l'article 6 de la loi n°2004-575 du 21 Juin 2004, seuls les Fournisseurs d'Accès Internet (FAI) étaient dans l'obligation expresse de mettre en place des outils de filtrage et d'archiver les données de connexions pendant une période d'un an. Désormais, ce présent article se voit étendu par la loi n°2006-64 du 23 janvier 2006 relative à la lutte contre le terrorisme et portant dispositions diverses relatives à la sécurité et aux contrôles frontaliers.

Ainsi, une société offrant un accès « public », se doit de mettre en place, au même titre qu'un FAI, une solution de filtrage et de conservation de données de connexions pendant une durée d'un an.

a) Utiliser le filtrage

Les juges étudient les usages des outils informatiques au sein d'une entreprise pour trancher lors d'un litige. Ceci donne un indice sur la pertinence et la récurrence d'un problème.

L'utilisation d'une solution de filtrage est aujourd'hui reconnue, voire indispensable, mais pour toutes les solutions, dites de sécurité, il est impératif de bien jauger entre sécurité et liberté.

Elle permet d'assurer un contrôle sur les actions effectuées par un individu dans le cadre professionnel – via des logs et fichiers – qui pourront dans certains cas, être utilisés pour sanctionner un abus.

Tout comme la législation européenne, le Droit français reconnait le terme de « filtre » ou de « filtrage » et fait référence à ces derniers par des terminologies ou notions comme « moyens techniques permettant de restreindre l'accès … » ou encore « procédure d'évaluation et de labellisation des moyens de sécurisation… ».

Dans un aspect juridique, il est impératif de comprendre le droit du filtrage, par conséquent celui des logs et des chartes d'usage des systèmes d'information.

Les Autorités Administratives Indépendantes, s'intéressent de très près au filtrage. C'est le cas de la CNIL, qui considère que limiter l'accès à Internet, ne vient en rien « bafouer » la vie privée des employés. L'accès à cet outil de communication ne doit – pour la CNIL – pas venir à l'encontre de la productivité générale de la firme et se doit de rester conforme aux « conditions d'accès professionnel au réseau ». Elle recommande, tout comme le fait l'HADOPI, d'opter pour un dispositif de filtrage, afin de veiller à ce que les employés ne viennent à se rendre sur des sites non autorisés faisant l'apologie du terrorisme, de racisme, de révisionnisme etc…

Dans la continuité, le droit de « logger » reste une conséquence directe de la mise en place d'une solution de filtrage. Il permet de créer des restrictions et/ou de contrôler les accès à des sites non autorisés. Il est également utilisé dans un objectif de surveillance individuelle et/ou collective d'Internet. Il est important de souligner que la CNIL qualifie d'élémentaire, de prévoir un système de journalisation (dont la période est de six mois de conservation) des actions des utilisateurs, des anomalies et des évènements liés à la sécurité.

Dans toute situation, le personnel se doit d'être informé de l'utilisation d'un outil de filtrage.

Après étude, la CNIL a jugé l'usage des keys loggers comme une atteinte excessive à la vie privée.

b) Ne pas utiliser de solution de filtrage

Comme nous venons de le souligner, il est fortement recommandé par les différentes autorités administratives, par la loi et la jurisprudence, de la nécessité du déploiement de solutions de filtrage. Dans le cas contraire, les risques que peuvent rencontrer une entreprise en n'optant pas pour un outil de contrôle sont de deux types :

- Ne pas respecter la loi ou être en contradiction avec une décision de justice ;
- Etre responsable des accès des autres, par conséquent, de leurs actions.

Article 6 Modifié par LOI n°2016-444 du 13 avril 2016 - art. 1

I.-1. Les personnes dont l'activité est d'offrir un accès à des services de communication au public en ligne informent leurs abonnés de l'existence de moyens techniques permettant de restreindre l'accès à certains services ou de les sélectionner et leur proposent au moins un de ces moyens. (…)

De manière indirecte, la LOI n°2004-575 du 21 juin 2004 art 6 I.-1° modifiée par LOI n°2016-444 du 13 avril 2016 – art. 1 pour la confiance dans l'économie numérique, impose aux abonnés (personne physique ou morale étant « juridiquement » liée à un Fournisseur d'Accès Internet (FAI)), l'obligation d'informer les utilisateurs de l'existence de moyens techniques pour restreindre les accès à Internet.

(..)II. Les personnes mentionnées aux 1 et 2 du I détiennent et conservent les données de nature à permettre l'identification de quiconque a contribué à la création du contenu ou de l'un des contenus des services dont elles sont prestataires.

De plus, le texte de loi cité précédemment, donne obligation aux personnes morales et physiques, de détenir et de conserver les données de nature à permettre l'identification des personnes qui viennent à se connecter sur leur réseau.

Notons que la responsabilité d'une entreprise peut être engagée sur les trois points suivants :

1. **L'article 1384 du code civil**
2. **L'article 121-2 du code pénal**
3. **L'article L336-3 du code la propriété intellectuelle**

Dans un plan jurisprudentiel, le 4 février 2005, la cour d'appel a rendu un arrêt, pouvant assimiler un employeur donnant un accès à ses employés à Internet, à un FAI. De fait, un employeur pourrait – en vue de cette interprétation de la loi – se voir opposer l'obligation légale de mettre à disposition des outils de filtrage et d'en informer les utilisateurs. Il se devra aussi de conserver les données d'identification comme cité dans le Décret n°2011-219 du 25 février 2011 relatif à la conservation et à la communication des données permettant d'identifier toute personne ayant contribué à la création d'un contenu mis en ligne. Dans un tout autre plan, le code de la propriété intellectuelle, représente un risque pour le titulaire d'accès de communication. En effet, celui-ci se doit de s'assurer que son accès ne soit pas utilisé à contrevenir aux droits de la propriété intellectuelle par des téléchargements illégaux d'œuvres protégées par le droit d'auteur. C'est pourquoi il est fortement recommandé l'usage d'outils de filtrage. Ce dernier code veille à renforcer l'obligation de filtrage des entreprises.

Article 1

Les données mentionnées au II de l'article 6 de la loi du 21 juin 2004 susvisée, que les personnes sont tenues de conserver en vertu de cette disposition, sont les suivantes :
1° Pour les personnes mentionnées au 1 du I du même article et pour chaque connexion de leurs abonnés :
a) L'identifiant de la connexion ;
b) L'identifiant attribué par ces personnes à l'abonné ;
c) L'identifiant du terminal utilisé pour la connexion lorsqu'elles y ont accès ;
d) Les dates et heure de début et de fin de la connexion ;
e) Les caractéristiques de la ligne de l'abonné ;
2° Pour les personnes mentionnées au 2 du I du même article et pour chaque opération de création :
a) L'identifiant de la connexion à l'origine de la communication ;
b) L'identifiant attribué par le système d'information au contenu, objet de l'opération ;
c) Les types de protocoles utilisés pour la connexion au service et pour le transfert des contenus ;
d) La nature de l'opération ;
e) Les date et heure de l'opération ;
f) L'identifiant utilisé par l'auteur de l'opération lorsque celui-ci l'a fourni ;

B. L'aspect légal des Chartes Informatiques

Article L1121-1
Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché.

Une charte Informatique est associée, en règle générale, comme une annexe du règlement intérieur, et a pour objectif d'établir les règles d'emploi de matériel, service informatique et Internet par les salariés, au sein de leur milieu professionnel. Elle est une limite aux usages abusifs des outils mis à la disposition du personnel.

Au même titre qu'un règlement intérieur, elle se doit d'être soumise à l'avis du comité d'entreprise ou d'établissement ou des délégués du personnel. Ensuite, elle devra faire l'objet d'un dépôt au greffe du conseil de prud'hommes et être communiquée à l'inspection du travail (Article R1321-1 Modifié par Décret n°2016-1417 du 20 octobre 2016 - art. 2). Pour la Jurisprudence elle représente une valeur juridique.

La charte permet notamment de lister :

- Toute solution de surveillance et de contrôle mise en place par l'employeur ;
- Les sites interdits (traitant de racisme, de révisionnisme, de terrorisme…) ;
- Le rappel sur l'interdiction et les sanctions d'usurpation d'identité d'autrui (en communicant ou en obtenant les accès d'un autre) ;
- Les sanctions en cas de non-respect des règles ci-stipulées (comme le licenciement) ...

Enfin, une charte informatique se doit d'être communiquée dans les meilleurs délais, à la connaissance d'un employé. Elle peut être ratifiée et datée par ce dernier pour le savoir au courant des règles et sanctions.

Article L336-3 Modifié par LOI n°2009-1311 du 28 octobre 2009 - art. 10

La personne titulaire de l'accès à des services de communication au public en ligne a l'obligation de veiller à ce que cet accès ne fasse pas l'objet d'une utilisation à des fins de reproduction, de représentation, de mise à disposition ou de communication au public d'œuvres ou d'objets protégés par un droit d'auteur ou par un droit voisin sans l'autorisation des titulaires des droits prévus aux livres Ier et II lorsqu'elle est requise.

Le manquement de la personne titulaire de l'accès à l'obligation définie au premier alinéa n'a pas pour effet d'engager la responsabilité pénale de l'intéressé, sous réserve des articles L. 335-7 et L. 335-7-1.

HADOPI préconise, elle aussi, une charte pour y faire mention de l'interdiction de la contrefaçon (en vue de l'article L336-3 modifié par LOI n°2009-1311 du 28 Octobre 2009 – art.10 du code de la propriété intellectuelle).

C. Protection des données personnelles

Article 2 Modifié par Loi n°2004-801 du 6 août 2004 - art. 1 JORF 7 août 2004

Constitue une donnée à caractère personnel toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne.

La loi informatique et liberté prévoit les grands principes sur la collecte, le traitement et la conservation de données à caractère personnel au sein des entreprises. Cette même loi est cautionnaire d'un certain nombre de droits pour les personnes concernées.

Ces privilèges seront, pour une personne désignée, « **le responsable de traitement** », des accès aux données « sensibles ». Il sera sous l'obligation formelle, avant tout emploi, d'annoncer au préalable les objectifs, appelés « finalités ». Cette annonce aura pour conséquences de limiter dans le temps, le traitement et l'utilisation de ces fichiers. Il fixera, par conséquent, une limite de conservation, en prenant en considération les éventuelles obligations à conserver certaines données.

Cependant, la collecte d'informations se doit de strictement respecter les objectifs précédemment établis, et ce, en faisant attention au caractère sensible de certains fichiers. D'ailleurs, selon le niveau de confidentialité de certaines informations, le responsable se doit de s'assurer qu'aucune personne non habilitée ne puisse accéder à ces dernières.

⇨ Les cas particuliers

Nous tenons à préciser que le nouveau règlement européen relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement général sur la protection des données : « RGPD ») paru au journal officiel de l'Union Européen (UE) entrera en application à compter du 25 mai 2018. Il poursuit trois objectifs :

- Renforcer les droits des personnes
- Responsabiliser les acteurs traitant des données
- Crédibiliser la régulation

Ce dernier s'applique sur :

- Les administrations
- Les grands groupes
- Les PME
- Les startups

A compter de cette date, bon nombre de formalités viendront à disparaitre, laissant place à une plus grande responsabilité des organismes. Ils devront par conséquent, assurer une protection optimale des données en temps réel et devront pouvoir être en mesure de démontrer leur conformité.

Au final, il est nécessaire d'effectuer les quatre points recommandés par la CNIL :

- **« Réaliser l'inventaire des traitements de données personnelles mis en œuvre ;**
- **Evaluer leurs pratiques et la mise en place des procédures (notification des violations de données, gestion des réclamations et des plaintes, etc…) ;**
- **Identifier les risques associés aux opérations de traitement et la prise en compte des mesures nécessaires à leur prévention ;**
- **Maintenir une documentation assurant la traçabilité des mesures. »**

II. Sécurisation des données

La sécurisation des données est un des enjeux essentiels. Un défaut de sécurisation peut entrainer des conséquences économiques et légales dramatiques pour l'entreprise.

A ce jour, la société AutoConcept ne présente pas une sécurisation des données suffisante car ils ont constaté des fuites de données et des pertes de données. Afin de palier à cela, la mise en place d'un plan de sécurisation des données est nécessaire. Ce plan devra comporter plusieurs volets et pouvoir couvrir la majorité des risques pouvant entrainer une fuite ou une perte de données.

⇨ ISO/CEI 27002

La norme ISO/CEI 27002 est une norme internationale portant sur la sécurité de l'information. De la même manière qu'ITIL apporte un référentiel de bonnes pratiques du management du système d'information, cette norme représente un ensemble de bonnes pratiques concernant la sécurité de l'information.

Même si elle n'est pas obligatoire, elle apporte un gage de qualité et permet de montrer le respect des bonnes pratiques en matière de sécurité.

Elle a pour objectif d'apporter une série de contrôles concernant les risques de sécurité liés à la confidentialité, l'intégrité et la disponibilité du système d'information. Ainsi, cette norme est le plus souvent utilisée de manière consultative afin de répondre à une problématique remontée lors d'une analyse de risques.

Elle se compose de 18 chapitres :

- Les 3 premiers chapitres concernent l'introduction et la présentation de la norme.
- Les chapitres 4, 5 et 6 sont en rapport avec l'aspect organisationnel allant de l'évaluation des risques à l'organisation de la sécurité de l'information.
- Le chapitre 7 porte sur les ressources humaines et concerne l'organisation de la sécurité liée aux collaborateurs.

- Du chapitre 8 au chapitre 11, la norme traite de la gestion des actifs, de la classification de l'information, du contrôle de l'accès au système d'information, de la cryptographie et de la sécurité physique et environnementale.
- Les chapitres 12 et 13 sont en rapport avec la sécurité liée à l'exploitation et la sécurité des communications, et représentent un des points essentiels de la sécurité quotidienne dans l'entreprise.
- Le chapitre 14 traite de l'évolution du système d'information, que cela soit au niveau logiciel ou matériel.
- Le chapitre 15 représente un aspect primordial pour notre entreprise, car il concerne directement la relation avec les fournisseurs et les prestataires de services.
- Les chapitres 16 et 17 concernent la gestion et le traitement des incidents, ce qui englobe également les plans de continuité et de reprise d'activité.
- Enfin le chapitre 18 porte sur l'aspect légal et la mise en conformité de l'entreprise vis-à-vis de la législation en vigueur.

⇨ ANSSI

L'ANSSI, ou Agence nationale de la sécurité des systèmes d'informations est un service à compétence nationale rattaché au secrétaire général de la défense et de la sécurité nationale.

Afin de garantir la sécurité des données, l'ANSSI préconise « dix règles de base »[2] à respecter. Ces règles sont présentées comme « les 10 commandements de la sécurité sur l'Internet ».

En voici un résumé :

- L'utilisation de mots de passes sécurisés difficiles à deviner et difficiles à trouver par des logiciels automatisés.
- Maintenir ses logiciels et système d'exploitation à jour.
- Effectuer des sauvegardes régulières
- Désactiver par défaut des composants annexes qui peuvent présenter des risques de sécurité, tel que Javascript, et ne les activer qu'en cas de besoin.

[2] Source : http://www.ssi.gouv.fr/entreprise/precautions-elementaires/dix-regles-de-base/
Les règles complètes sont présentées dans l'annexe 3.

- Etre vigilant avant de cliquer sur un lien.
- Utiliser un compte simple et non un compte administrateur pour les usages quotidiens.
- S'assurer de l'utilisation faite des données personnelles avant de les communiquer.
- Faire attention à nos actions et ne pas envoyer ou relayer des messages et informations inutiles.
- Etre prudent et appliquer des mesures de précautions en essayant au maximum de vérifier les informations.
- Ne jamais ouvrir de pièces jointes sans être sûr de la provenance et s'il n'y a pas de possibilité de vérifier n'ouvrir que les fichiers les moins à risque.

⇨ Plan de sécurisation des données

La mise en place de ce plan doit pouvoir permettre à AutoConcept de limiter les risques et de pouvoir assurer la production en continu.

A. Enjeux

Les enjeux principaux du plan de sécurisation des données seront :

- D'assurer la disponibilité du système d'information
- D'assurer l'intégrité des données
- D'assurer la confidentialité des données
- D'assurer l'identification des utilisateurs et de pouvoir tracer leurs actions

B. Conséquences

Les principales conséquences liées à la non sécurisation des données sont les pertes financières directes ou indirectes survenant à la suite d'un piratage ou d'un incident.

Une autre conséquence repose sur l'image de marque et l'image de fiabilité dégagée par l'entreprise. En effet, cela peut avoir des conséquences désastreuses et faire fuir des clients si leurs données ne sont pas sécurisées.

C. Risques

Il convient d'analyser les différents risques afin de pouvoir proposer des solutions concrètes qui seront formalisées dans le plan de sécurisation des données.

On peut distinguer en sécurité trois grands facteurs :

- La sécurité humaine, qui prend en compte les facteurs de risques liés aux individus.
- La sécurité matérielle, qui prend en compte la sauvegarde des données, leur réplication et aussi l'environnement dans lequel les données sont stockées.
- La sécurité logicielle, qui prend en compte les attaques pouvant impacter le système d'information.

⇨ AutoConcept

A ce jour, les principaux incidents que rencontre la société AutoConcept peuvent être classés dans les trois facteurs de sécurité.

En reprenant toutes les informations présentées, nous pouvons dresser un plan de sécurisation des données pouvant répondre aux problématiques rencontrées.

Plan de sécurisation des données

L'architecture de ce plan peut reprendre les grands chapitres de la norme ISO/CEI 27002, cela va permettre de le dérouler de manière efficace en s'appuyant sur un référentiel reconnu.

- Il conviendra de faire une évaluation des risques, en prenant en compte les retours fournis par le service commercial. A la suite de cela, il faudra définir une politique de sécurité ainsi qu'un cadre d'évaluation afin de l'améliorer en continu. La partie organisationnelle sera essentielle afin de clarifier les responsabilités au sein de l'entreprise.

- Afin de pallier aux risques liés à la sécurité humaine, il faudra définir des mesures accompagnant le collaborateur avant, pendant et après sa collaboration avec l'entreprise.

Dans le but d'aider à cette tâche, une classification de l'information sera essentielle et permettra d'identifier aisément qui doit avoir accès à quoi. Ainsi, avec le contrôle des accès à l'information, AutoConcept se protègera de manière plus efficace des fuites de données.

- Pour renforcer encore plus cette composante, le recours à des solutions de cryptage permettra de sécuriser davantage les données sensibles. En fonction du matériel choisi par l'entreprise comme solution de sauvegarde, le cryptage pourra être fait de manière automatique contre les intrusions extérieures. Afin de sécuriser les données contre les fuites internes, le recours à une deuxième solution de cryptage en supplément peut être intéressant. Cela peut se traduire par des archives de type .zip ou .rar encryptées.

- D'un point de vue matériel et dans l'optique d'éviter toute intrusion ou incident physique sur les machines, une sécurisation des locaux techniques et publics sera essentielle. L'infrastructure sécurisée est un élément clé pour limiter les risques de pertes de données.

- D'un point de vue logiciel, il est nécessaire de sécuriser les périodes d'exploitation et de sécuriser les communications. Ainsi, l'utilisation d'une solution antivirus, la mise en conformité des licences, le filtrage et la mise en place de procédures limiteront les risques liés à l'exploitation.

- Le dernier point du plan de sécurisation concerne la gestion des incidents. Il conviendra de définir les différents types d'incidents possibles et de définir une procédure pouvant répondre aux différents cas de figure présentés. Dans le cas où un cas inconnu se présente, il faudra que les personnes en responsabilité soient formées et puissent proposer des solutions permettant d'y faire face, ou à défaut de préparer des procédures prenant en compte les problématiques afin de pouvoir y répondre, par la suite, de manière efficace.

- Enfin, l'élaboration d'un plan de continuité d'activité (PCA) et d'un plan de reprise d'activité (PRA) permettront, en dernier recours, à AutoConcept de pouvoir limiter les pertes et reprendre une production le plus rapidement possible. L'objectif de ces plans se présente comme ceci :

- Le PCA a pour but de permettre à l'entreprise de redémarrer son activité le plus rapidement possible à la suite d'un incident n'ayant pas complètement stoppé la production. Ainsi lors de l'élaboration du plan de sécurisation des données, le PCA représente la suite de procédures à mettre en œuvre.
- Dans le cas d'une crise majeure entrainant un arrêt total de la production, le PCA ne sera pas suffisant et l'élaboration d'un PRA sera un des éléments essentiels à la survie d'AutoConcept. Ce plan a pour but d'organiser les procédures pouvant aller jusqu'à la reconstruction de l'infrastructure et la remise en service du système d'information.

Chaque plan doit contenir des mesures préventives et des mesures correctives. Cela se traduit par une démarche proactive via une analyse des risques et une maintenance continue du parc matériel et logiciel. Les mesures correctives consistent à appliquer des procédures visant à restaurer le système d'information et peuvent inclure la souscription à des assurances.

Sécuriser à 100% le système d'information d'AutoConcept est une tâche illusoire. Cependant en appliquant toutes ces mesures, l'entreprise sera en mesure de pouvoir répondre à différents cas de figure et ainsi limiter les risques liés à la perte de données.

III. Sauvegarde

La société AutoConcept ne présente à ce jour pas de plan de sécurisation des données. Or, la sauvegarde des données est un des enjeux majeurs des entreprises.

Au-delà de l'aspect purement financier de la perte des données, cela peut avoir un impact non négligeable sur la production d'une entreprise. En effet, pendant le temps où les données sont indisponibles, les salariés voient leur travail perturbé voire complétement interrompu. Pendant ce temps les salaires ainsi que les coûts liés au fonctionnement de l'entreprise ne s'arrêtent pas.

⇨ Définition d'un plan de sauvegarde des données

Définir un plan de sauvegarde des données devient un impératif pour toute entreprise car cela permet d'éviter les pertes directes, mais permet aussi une reprise d'activité dans les plus brefs délais. AutoConcept aurait pu ainsi éviter les pertes d'exploitation de 80000€ et 60000€ mais aussi les coûts cachés liés au temps pour reprendre et recommencer le travail tout en le menant à bien.

Pour mieux prévenir les pertes de données il faut en premier lieu déterminer les principales causes de pertes :

Les défaillances matérielles

Afin de prévenir les défaillances matérielles le choix des composants ainsi que l'architecture du système de sauvegarde permettent dans la plupart des cas de sécuriser les données.

Les sinistres

Pour éviter les sinistres, la solution principale reste la délocalisation des données dans un lieu externe à l'entreprise. Cela permet d'éviter la perte des données ainsi que de toutes les sauvegardes en même temps.

Les actes malveillants causés par des tiers

Les actes malveillants causés par des tiers peuvent être évités par une sécurisation du système d'information ainsi que des sauvegardes délocalisées. Les « ransomwares » sont aujourd'hui une des principales menaces pour les entreprises.

Les actes malveillants causés par des personnes internes

Pour éviter les pertes liées à des personnes internes, la codification et classification des données en restreignant l'accès permet de protéger les données les plus sensibles. Les sauvegardes régulières ainsi que la délocalisation permettent dans la plupart des cas d'éviter une perte totale des données.

⇨ Plan de sauvegarde des données pour AutoConcept

Après avoir identifié les risques puis cerné les principales causes de perte de données, il faut maintenant dresser un inventaire des données présentes et établir un prévisionnel des besoins afin de déployer un système de sauvegarde en adéquation avec les besoins d'AutoConcept. Le système proposé doit ainsi s'intégrer au fonctionnement de l'entreprise, être sécurisant mais ne pas devenir gênant pour la production.

Les postes des utilisateurs n'étant pas sécurisés, la récupération et l'analyse des données sur un poste sécurisé va permettre la « désinfection » des données et engager le travail de classification. Cette première sauvegarde va permettre de sécuriser les données et lancer la suite de la procédure.

En fonction du volume de données déjà présentes et de la prévision de leur augmentation, le plan de sauvegarde va pouvoir être établi.

Plusieurs solutions allant d'un disque dur externe à un serveur peuvent être envisagées. Ici l'offre la plus cohérente est le Network Attached Storage (NAS) qui a l'avantage de présenter

un système "clés en main" facile à déployer et maintenir, tout en présentant des fonctionnalités intéressantes.

En plus des fonctionnalités de sauvegarde automatique, la compatibilité avec différents systèmes d'exploitation, la gestion des comptes et groupes utilisateurs, l'accès à distance aux données, les sécurités proposées (chiffrage des données, antivirus intégré), la faible consommation et le faible encombrement en font un outil efficace et évitant l'achat et les coûts liés à l'exploitation d'un serveur.

Cependant un NAS tout seul ne présente pas une sécurisation suffisante, car il ne couvre pas tous les scénarios possibles de pertes. Afin de se prémunir du risque lié aux sinistres et de pouvoir déporter les données hors de l'entreprise, plusieurs solutions s'offrent.

- La première consiste à sauvegarder les données sur un disque dur externe qui sera amené hors de l'entreprise ou mis en sécurité dans un coffre-fort. Cette solution présente un avantage de coût intéressant mais présente certains risques comme la perte du disque ou la casse de celui-ci. La responsabilité repose ainsi sur le directeur ou un salarié désigné augmentant de ce fait les risques encourus pour les données.
- La deuxième solution consiste à se servir d'un service dans les nuages ou cloud. L'avantage de ce système est qu'il assure une disponibilité des données en permanence. Le principal inconvénient est la dépendance à une connexion internet fiable et rapide pour pouvoir accéder aux sauvegardes. De même le fait de ne pas savoir où se situent les données peut présenter un frein à l'adoption d'un tel système.
- La troisième solution représente une solution hybride entre les deux premières, en achetant deux NAS de la même marque et en en installant un dans un lieu externe à l'entreprise. Cela revient presque à doubler le coût à l'achat mais présente un compromis intéressant en assurant une sauvegarde du premier NAS. Même si cette solution semble récupérer les inconvénients des deux autres solutions, elle limite au maximum les risques rencontrés par les deux autres solutions.

- **Proposition de solutions de sauvegarde**

Il faudra proposer plusieurs solutions à la société AutoConcept pouvant répondre aux besoins de sécurisation et de sauvegarde des données. Chaque solution présentée ici représente un degré de sécurisation associé à une notion de coût.

✓ La première solution consiste en l'achat et l'installation d'un NAS sur site afin d'assurer une sauvegarde des données présentes sur chacun des postes. Cela implique l'utilisation d'un logiciel de sauvegarde ainsi que l'achat d'un disque dur externe afin de procurer une solution de sauvegarde plus complète. A minima un NAS contenant deux baies, dans l'idéal un NAS à cinq baies.

Voici quelques exemples de NAS pouvant convenir :

- Pour les NAS deux baies, le Synology DS218+ et le Qnap TS-253B
- Pour les NAS cinq baies, le Synology DS1517+ et le Qnap TS-563

A ces NAS, il faudra adjoindre de deux à cinq disques durs adaptés en fonction des besoins en stockage et permettant de faire plusieurs sauvegardes garantissant un retour en arrière sur plusieurs jours. Les disques devront être configurés en RAID 1 au minimum et idéalement en RAID 5[3] ou 6[4].

Concernant le logiciel de sauvegarde celui-ci peut être intégré à Windows comme l'outil de sauvegarde ou être une solution tierce telle que Cobian Backup.

Le disque dur externe devra être de capacité suffisante afin de permettre une sauvegarde des données et de pouvoir les transporter à l'extérieur de l'entreprise.

Cette solution a l'avantage de proposer une offre complète proposant des coûts limités sur la durée. L'investissement au départ sera vite rentabilisé sur la durée mais en contrepartie cela implique une plus grande responsabilité de la personne en charge de la

[3] Le RAID 5 doit être composé d'au moins trois disques idéalement de même capacité et tolère la panne d'un disque. La capacité totale de stockage se calcule selon cette formule : (nombre de disques - 1) x (capacité du disque le plus petit).
[4] Le RAID 6 est similaire au RAID 5 à la différence qu'il tolère la panne de deux disques durs et la capacité totale de stockage se calcule selon cette formule : (nombre de disques - 2) x (capacité du disque le plus petit).

gestion du disque dur externe. De même, le fait que les données soient hébergées en local sur chaque machine présente un risque supplémentaire de pertes de données entre les sauvegardes programmées.

- ✓ La deuxième solution reprend l'achat d'un NAS similaire à celui proposé dans la première solution. La différence va se jouer dans l'utilisation des offres dans les nuages afin de remplacer la sauvegarde sur le disque dur externe. L'utilisation de cette solution dépendra en grande partie de la connexion internet disponible au sein des locaux d'AutoConcept. Le débit montant et le débit descendant seront le principal facteur limitant.

  Voici quelques exemples d'offres de stockage dans les nuages :

  - Google Cloud Platform propose des solutions de stockage basées sur une facturation à l'utilisation. Le coût de stockage est de 0.02 dollars par Go de données par mois. Cela représente environ 1500€ par an pour 5To de données.
  - Microsoft Azure propose des solutions de stockage similaires à celle de Google Cloud Platform. Le coût de stockage est de 0.0166€ par Go de données jusqu'à 50To par mois. Le prix est dégressif passé ce seuil. Cela représente environ 1000€ par an pour 5To de données.

  Cette solution permet de compenser les risques liés à l'utilisation d'un disque dur externe, tout en rendant l'accès aux données possible depuis n'importe quel lieu. En revanche cela représente un coût non négligeable sur la durée et impose de posséder une connexion rapide.

- ✓ La troisième solution est celle reprenant l'utilisation de deux NAS de la même marque et possédant une capacité de stockage similaire mais disposés en deux endroits différents. Cela représente un coût important à l'achat mais permet d'être moins coûteux sur la durée que la deuxième solution, tout en limitant les risques liés à la première.

  Même si les deux NAS doivent être de la même marque pour des soucis de compatibilité et de facilité de paramétrage, le NAS déporté dans un autre lieu n'a pas besoin d'être exactement le même modèle. Ainsi, il est possible d'installer un NAS 5 baies dans l'entreprise et d'installer un NAS 2 baies ailleurs.

Cette troisième solution peut être modifiée afin de proposer un hébergement des données de sauvegarde dans nos locaux sur nos serveurs ou dans un NAS dédié à l'entreprise. Cela permet de décharger la responsabilité de la personne en charge d'accueillir le NAS déporté, tout en permettant à notre entreprise de proposer un service supplémentaire.

Ces solutions représentent des solutions faciles à déployer et à maintenir tout en garantissant une sécurité optimale et en limitant les risques liés aux pertes de données. Il est tout à fait possible de proposer à AutoConcept une solution complète reprenant toutes les possibilités de sauvegarde décrites au-dessus mais cela représenterait un coût trop important associé à un système de sauvegarde surdimensionné par rapport à la taille de l'entreprise.

- **Cloud**

En association avec ces propositions, il est également possible de conseiller à AutoConcept d'envisager les solutions professionnelles de stockage individuel et de travail collaboratif proposées par diverses sociétés comme Google et Microsoft.

- La solution de Google G Suite propose pour 10 dollars par mois et par utilisateur des adresses mails professionnelles associées à un système de visioconférence, des calendriers partagés, le partage de documents, l'accès à la suite bureautique de Google et un stockage illimité dans les nuages.
- La solution de Microsoft Office 365 Business Premium propose pour 10,50€ par mois et par utilisateur les mêmes possibilités que l'offre de Google avec pour différence la limitation à 1To de stockage dans les nuages et la suite de logiciels Office 2016.

Cela permet de mettre à disposition des collaborateurs d'AutoConcept des logiciels bureautiques associés à une capacité de stockage importante. Ainsi les données, en plus d'être sécurisées, peuvent être partagées et utilisées sur n'importe quel ordinateur. Une solution professionnelle de ce type présente un certain coût sur la durée mais présente des avantages de productivité intéressants, tout en étant entièrement compatible avec les solutions de sauvegarde des données présentées en amont.

IV. Infogérance

⇨ Introduction

Cette note de synthèse a pour objectif d'accompagner l'entreprise AutoConcept dans leur transition vers une gestion différente de leur système d'information.

Le premier objectif est d'assurer une transition de leur système d'information vers un fonctionnement plus sécurisé tout en leur apportant des améliorations notables.

Le deuxième objectif consiste à leur proposer un contrat de maintenance et de support sur plusieurs années leur permettant de continuer leur activité sans que le système d'information ne soit un frein à leur productivité.

Ainsi, nos actions et nos engagements seront annexés au contrat de maintenance et de support sous la forme d'une charte « Qualité Service Client ».

⇨ Transition

Aujourd'hui, la société AutoConcept compte entre 70 et 80 postes dans leur parc informatique. Ils ont deux techniciens embauchés en interne qui assurent le support et la maintenance.

Cependant, nous pouvons constater plusieurs problèmes dans le fonctionnement actuel :

- D'un point de vue matériel et logiciel, la rapidité et l'efficacité de la maintenance ne semble pas être optimale car cela engendre un impact sur la productivité de l'entreprise.
- Concernant le support et la gestion des incidents, cela ne semble pas être efficace ni organisé.
- L'utilisation d'un référentiel de bonnes pratiques ainsi que le management des techniciens ne semble pas être mis en place.

La première étape va être la formalisation écrite d'une charte informatique et une mise en conformité légale afin que l'entreprise soit protégée, protège son activité et ses salariés.

La deuxième étape concernera la mise en place d'une stratégie du système d'information afin de rationaliser les processus et mettre en place des procédures. Cela va mener l'entreprise dans une logique d'optimisation de l'utilisation des technologies de l'information et facilitera la création des procédures permettant la mise en place d'un plan de sécurisation des données, d'un PCA et d'un PRA.

La troisième étape concernera les actions d'infogérance, allant de la modernisation du système d'information à la maintenance et le support sur le long terme.

⇨ Modernisation du système d'information

Préalablement au démarrage de la modernisation du système d'information, le recrutement d'un des deux techniciens présents sur le site semble être un atout non négligeable. En effet, sa connaissance de l'entreprise permettra une mise en action rapide.

Cependant, dans le cas où le processus de recrutement serait long et la formation de la personne au fonctionnement de notre entreprise difficile, il se peut qu'il n'intervienne pas immédiatement dans le processus de transition.

Après avoir rédigé le plan de sécurisation des données, nous pourrons démarrer la sécurisation des postes informatiques et déployer le système de sauvegarde choisi.

Le plan de sécurisation des données comprendra la mise en conformité des licences logicielles, le recours à une politique de mots de passe sécurisés, l'utilisation d'une solution antivirus et le choix d'une solution de sauvegarde des données.

Afin de pouvoir accélérer le déploiement et de rendre la transition rapide, la création d'un ou plusieurs « ghost » ou « master » en fonction des spécificités logiciels permettra de déployer rapidement sur la totalité des postes informatiques un système sain et prêt à l'emploi. Dans le cas où le recours à un « ghost » ou « master » ne serait pas possible nous procéderons à une réinstallation des postes le plus rapidement possible. Par la suite, le fait d'avoir des images

prêtes à l'emploi permettra le redéploiement d'un poste rapidement, réduisant ainsi la perte de productivité.

Par la même occasion, nous procéderons à un diagnostic matériel des postes présentant des problèmes afin de déterminer si un redéploiement sera suffisant ou si des réparations et un changement de matériel sont nécessaires.

La réinstallation des logiciels métiers sera si possible intégrée au « ghost » ou « master ». Si cela s'avère impossible nous procéderons à une réinstallation manuelle.

Le but de cette étape sera de générer des outils permettant d'industrialiser les processus de déploiement et de redéploiement afin de pouvoir proposer des engagements réalistes par la suite.

⇨ Maintenance et support

Une fois le parc informatique redéployé et l'application de la procédure de sécurisation des données mise en place, nous pourrons entrer dans la phase de maintenance et de support.

Afin de permettre une administration optimisée, nous conseillerons d'utiliser les fonctionnalités de contrôleur de domaine[5] intégrées au sein des NAS proposés dans le plan de sécurisation des données. Ainsi, nous pourrons nous occuper de l'administration des comptes et de la gestion de la sécurité de manière efficace. Cela permettra aux techniciens du support de pouvoir réinitialiser les mots de passes des utilisateurs et de contrôler de manière précise l'accès aux données au sein du système d'information.

Le support utilisateur sera effectué à distance ou sur place par notre équipe technique via notre portail de création d'incident et via notre ligne téléphonique. Le technicien d'AutoConcept embauché pourra devenir un des interlocuteurs privilégiés de l'entreprise. De même, suivant la distance et afin de garantir la réactivité et la disponibilité en cas d'incident, nous pourrons détacher un technicien sur place pour qu'il assure le support et la maintenance en direct.

[5] Un Domaine définit un ensemble de machines partageant des informations d'annuaire.

D'un point de vue matériel, nous préconiserons à AutoConcept d'avoir au sein de leurs locaux un stock de matériel de rechange suffisant, afin de pouvoir procéder à un échange du matériel défectueux. La réparation permettra par la suite de remettre le matériel défectueux dans le stock. Nous proposerons un système d'inventaire, que nous pourrons gérer en interne, pour garder un contrôle sur le matériel utilisé et disponible. Lors d'un incident, la reprise de l'activité s'en trouvera grandement accélérée.

⇨ Conseils et gestion de projet

Nous nous efforcerons d'être un acteur essentiel dans l'utilisation et dans la stratégie d'évolution du système d'information d'AutoConcept. De même, nous assurons une veille technologique et juridique afin d'être pertinents dans nos conseils.

Notre objectif sera de proposer, pour chaque besoin ou projet, notre expertise et notre savoir-faire afin de conseiller et d'accompagner AutoConcept dans chaque étape de l'évolution du système d'information. Cela pourra se traduire par l'élaboration, la mise en œuvre et l'analyse d'un projet ou par des conseils dans l'utilisation du système d'information.

⇨ Démarche qualité

Dans le cadre de notre démarche qualité nous garantissons plusieurs points permettant d'apporter un service professionnel de qualité.

La formation continue des techniciens est un des points essentiels, car cela permet de proposer une expertise lors de chaque intervention. Cela inclut la veille technologique et juridique, mais aussi les certifications et formations suivies par chaque technicien.

Dans le cadre du recrutement d'un des techniciens d'AutoConcept, ce dernier va être évalué au niveau de ses compétences et nous lui proposerons une ou des formations afin qu'il atteigne nos standards de qualité.

La démarche ITIL nous permet de nous appuyer sur un référentiel reconnu à l'échelle internationale afin de proposer un service optimal. Grace à cela nous avons pu mettre en pratique un mémo interne afin de normaliser un standard de qualité vis-à-vis du traitement des incidents et de l'accompagnement de nos clients.

De même, avec la mise en place d'enquêtes de satisfaction nous pouvons avoir un retour en temps réel concernant nos prestations et ainsi pouvoir ajuster nos actions en fonction des critiques reçues.

Un autre point essentiel de notre démarche qualité est la relation de confiance que nous développons avec nos clients. Afin d'être un partenaire dans la croissance de leur entreprise, la confiance est un des critères majeurs de notre démarche qualité. Cela passe par l'application stricte de règles de confidentialité, mais aussi par une transparence vis-à-vis de nos actions au quotidien. Lorsque que nous intervenons, nous nous efforçons de détailler nos actes dans un jargon compréhensible et clair.

⇨ Formation

Dans le cadre des changements effectués, nous veillerons à une transition en douceur vis-à-vis du personnel d'AutoConcept. Un accompagnement sera effectué dans le cadre de la mise en place de la Charte Informatique notamment, afin de rappeler au personnel les conditions d'utilisation du système d'information. Les solutions mises en place doivent être clairement expliquées à chacun afin d'éviter des réticences et une baisse de productivité due à une mauvaise assimilation des systèmes mis en place.

Nous proposerons donc une réunion d'information préalable au déploiement de toutes les solutions au cours de laquelle nous présenterons notre société et nous rassurerons les employés concernant la transition. Lorsque les solutions de sauvegarde et de sécurisation seront effectives, nous organiserons alors une ou plusieurs sessions de formation, par groupes, afin de développer les sujets de la charte informatique et de la gestion d'incidents principalement.

Un compte rendu de ces sessions de formation sera rédigé en tenant compte des réactions et des questions du personnel, et pourra ainsi être conservé au sein de l'entreprise AutoConcept, afin de le présenter lors des embauches ultérieures.

Sur la durée, de nouvelles formations pourront se révéler nécessaires lors de l'analyse des incidents effectuée dans le respect des bonnes pratiques ITIL. En effet, lorsqu'un type d'incident devient récurrent, son analyse pourra révéler des erreurs de manipulation fréquentes des utilisateurs. Il sera alors mis en place une solution dans le but de réduire les incidents récurrents, cette solution pouvant être la nécessité d'une nouvelle formation dispensée aux utilisateurs.

La formation a donc une importance capitale dans nos rôles de conseil et de disponibilité et a une incidence directe sur notre charge de travail. Il faut donc rappeler l'importance de la communication lors de toutes les interventions réalisées. En expliquant pourquoi et comment nous intervenons sur un ou plusieurs postes, nous sensibiliserons les utilisateurs aux risques liés à l'utilisation de l'informatique en entreprise.

Dans cette perspective, toute évolution technologique ou juridique pertinente sera portée à la connaissance du personnel AutoConcept afin de faciliter notre collaboration.

⇨ Charte « Qualité Service Client »

La charte « Qualité Service Client » représente la formalisation écrite de nos engagements envers AutoConcept et sera annexée au contrat d'infogérance nous liant. Elle repose sur des principes et des valeurs fortement liés à notre vision du métier.

Charte Qualité Service Client de la société IDK

Chez IDK, la qualité et la satisfaction du client sont des exigences essentielles qui sont au cœur de notre activité. Notre engagement se traduit par ces principes :

1. Accueil : garantir la qualité de l'accueil sur place, à distance ou par téléphone.
2. Disponibilité : être disponible, réactif et à l'écoute des besoins.
3. Clarté : être clair et fournir des informations complètes, fiables et compréhensibles.
4. Personnalisation : apporter un service adapté aux besoins de l'entreprise.
5. Confidentialité : garantir la confidentialité des données tout en respectant la vie privée.
6. Compétence : garantir l'expertise des techniciens et apporter une vision professionnelle.
7. Contrôle qualité : assurer une démarche qualité en prenant en compte la législation en vigueur, les retours clients et en améliorant continuellement les services proposés.
8. Transparence : être transparent dans les actions, dans les devis et dans le fonctionnement.
9. Démarche ITIL : s'engager au quotidien dans la mise en œuvre des bonnes pratiques ITIL pour garantir un service optimal.

V. ITIL

Nous avons choisi de travailler en se basant sur le référentiel ITIL car il est aujourd'hui le plus complet et accessible. C'est également une démarche positive et décisive aux yeux de nos clients grâce à la notoriété acquise au fil des années par ITIL, aujourd'hui largement reconnu.

Pour cela, nous mettrons en avant cette démarche, qui est un gage de qualité et d'organisation afin de rassurer le client.

Pour chaque étape de la transition du service informatique d'AutoConcept, un processus ITIL existe et nous permettra une mise en place fiable et efficace.

Ainsi, ITIL recommande dans un premier temps la mise en place d'une CMDB (Configuration Management Data Base), dans laquelle tout le matériel ainsi que ses configurations seront répertoriés. Cette première étape, à la condition d'une mise à jour régulière, permettra de faciliter l'obtention d'un parc homogène et une visibilité globale sur le parc informatique.

Il est ensuite recommandé de mettre en place un guichet unique destiné aux utilisateurs. Cette étape consiste à faire respecter aux utilisateurs les procédures de requêtes ou de signalements d'incidents, afin que chaque demande soit consignée.

De cette manière, pour chaque demande, une fiche d'incident sera remplie, et dès que l'incident sera clôturé, une fiche de résolution lui sera attachée.

Grâce à l'association de ces contrôles, nous développerons le traitement réactif des demandes des utilisateurs, mais aussi un traitement pro-actif grâce à la visibilité du parc et à l'analyse des incidents répertoriés.

En étudiant le compte-rendu du service commercial d'AutoConcept, de nombreuses plaintes des utilisateurs pourraient être évitées par la mise en place de ces dispositifs.

- ✓ *Un utilisateur de l'atelier rapporte qu'il a dû insister auprès du service informatique pour retrouver son écran d'origine. Un écran plus petit lui avait été remis après une intervention.*

Ce genre d'erreur sera évité grâce à la CMDB, grâce à laquelle le suivi du matériel est facilité.

- ✓ *Un utilisateur du service commercial se plaint que son poste, après plusieurs séjours au SAV, présente toujours les mêmes symptômes.*
- ✓ *Un utilisateur du service "Véhicules d'occasion" se plaint depuis plusieurs mois d'avoir des problèmes avec sa souris. Personne n'a répondu à son problème.*

Chaque demande a son importance et chaque demande doit faire l'objet d'une fiche d'incident. Cela permettra de faire un travail de gestion des priorités, mais aussi de visualiser les incidents qui n'ont pas été résolus, et d'y remédier.

- ✓ *Délais d'intervention : un poste d'une secrétaire commerciale est parti en SAV durant 2 jours. Elle n'a pas pu terminer un document pour conclure une affaire. Perte : 60000 euros.*
- ✓ *Une intervention urgente planifiée le lundi à 10h a été traitée le mercredi à 10h.*
- ✓ *Une bonne partie des utilisateurs se plaignent de voir leurs postes partir en SAV sans savoir quand il reviendra.*

Les processus ITIL de gestion des incidents et de gestion de la disponibilité sont concernés dans ces cas. A chaque incident doit être associé un niveau de priorité associé à un délai de résolution. Si le technicien n'est pas capable de résoudre le problème, ou de respecter le délai, il devra escalader la demande dans un délai raisonnable. Il ne faut pas oublier également de communiquer avec l'utilisateur et de lui signaler les démarches effectuées et les solutions mises en œuvre.

- ✓ *Intrusion d'un client sur un poste d'une commerciale dépourvu de mot de passe.*
- ✓ *Messages intempestifs de "version de Windows pirates".*
- ✓ *Un utilisateur signale que son MSN ne fonctionne pas et souhaite que son poste soit réparé rapidement. (NB : la direction a demandé au service informatique de bloquer MSN. Depuis la productivité a considérablement augmenté).*

Chacun de ces incidents reflète la mauvaise utilisation de l'outil informatique par les employés et la nécessité de la mise en place d'une Charte Informatique afin d'informer les utilisateurs de leurs droits et devoirs.

- ✓ *Attitudes des techniciens : absence d'explication sur les interventions, ou parfois discours trop techniques.*
- ✓ *Tenue des informaticiens : "un matin, l'un d'eux est arrivé en jogging pour dépanner un poste alors qu'un commercial était avec un client". Un autre a répondu de manière déplacée à la demande d'un utilisateur de le dépanner.*
- ✓ *Un utilisateur de la comptabilité soupçonne le SAV d'avoir consulté des documents confidentiels sur son poste lors d'une intervention. Ces informations ont été divulguées à des tiers.*
- ✓ *Plusieurs utilisateurs se plaignent de l'accueil téléphonique du service informatique.*

Ces plaintes reflètent le manque de professionnalisme des informaticiens sur place et le manque de confiance des clients envers eux.

Il est essentiel d'instaurer une bonne communication entre tous les services et des relations cordiales et respectueuses.

En s'appuyant sur le compte-rendu des plaintes d'AutoConcept, nous proposons de diffuser un mémo à tous les employés de notre société, notamment aux nouveaux, afin de rappeler la conduite à tenir chez un client.

Mémo interne de bonnes pratiques

Le présent document a pour objet de rappeler les règles de discipline générale et de bonnes pratiques vis-à-vis de nos clients. Parce que nos relations et notre réputation en dépendent, ces bonnes pratiques s'imposent à tous les salariés, apprentis, stagiaires, en quelque endroit qu'ils se trouvent. Ils doivent s'y conformer sans restriction ni réserve.

Un exemplaire de ce document est communiqué à chaque nouveau salarié lors de son embauche.

- Discipline Générale
  - Horaires de travail

Les salariés doivent respecter les horaires qui leur sont communiqués. Ils doivent se trouver à leur poste, en tenue de travail, aux heures fixées pour le début et la fin du travail.

Tout retard ou absence doit être signalé dans un délai raisonnable au supérieur hiérarchique et/ou au client dans le cas d'une intervention.

  - Discipline

Il est formellement interdit à tout salarié :

- De se livrer à des travaux personnels sur les lieux de travail ainsi qu'à toute activité étrangère à son travail ou à sa fonction ;
- D'avoir une attitude discourtoise vis-à-vis de la clientèle, de la hiérarchie, des collègues de travail ;
- D'emporter sans autorisation écrite des objets, matériels, marchandises quelconques appartenant à l'entreprise ;
- D'introduire dans le système d'informations de l'entreprise des logiciels n'appartenant pas à l'entreprise, sans avoir obtenu pour cela une autorisation écrite. De même, aucune copie illicite ne devra être effectuée tant pour son propre usage qu'au bénéfice de l'entreprise.
- De copier ou de divulguer des informations personnelles ou confidentielles ;
- D'introduire sur le lieu de travail des personnes étrangères au service ;

- D'utiliser les moyens de communication à des fins personnelles.

❖ Professionnalisme

➢ Tenue de travail

Le personnel est tenu de se présenter sur son lieu de travail en tenue correcte et propre. Le port du badge doit être systématique lors d'une intervention chez un client afin que ce dernier puisse identifier le technicien et l'entreprise.

➢ Courtoisie

Le respect, la politesse et l'esprit d'équipe sont de rigueur. Quels que soient l'interlocuteur et la demande, il conviendra de se montrer calme, patient et serviable. Le discours tenu doit être adapté à l'interlocuteur afin de se faire comprendre de tous.

➢ Organisation

Chaque intervention doit être effectuée dans le respect des procédures. La gestion des priorités est la clé d'un travail serein et efficace.

L'utilisateur doit être systématiquement informé lors d'une intervention sur son poste de travail, de la nature et de la durée des manipulations effectuées.

➢ Confidentialité

Le personnel est tenu de garder une discrétion absolue sur tout ce qui a trait aux travaux exécutés, aux statistiques, aux relations avec les clients. Il doit s'assurer du respect de la confidentialité lors des interventions et ne doit accéder à un poste de travail ou à des fichiers qu'après autorisation de l'utilisateur.

➢ Pédagogie

Le personnel pourra être amené à constater des manquements au respect de la charte informatique. Dans de telles circonstances, il conviendra de rappeler à l'ordre les utilisateurs en faisant toujours preuve de courtoisie et de pédagogie. Une mauvaise utilisation des outils informatiques et les failles de sécurité auront une incidence directe sur le travail de nos équipes. Le personnel se doit donc de respecter et de faire respecter la charte informatique.

VI. Conclusion

AutoConcept est, de par la gestion actuelle de son système d'information, dans une situation délicate. L'absence de direction à ce niveau est dommageable à sa production.

L'essentiel de notre travail va être de pallier à ce manque en leur proposant un plan de sécurisation des données et une mise en conformité légale, mais aussi en leur conseillant l'utilisation des bonnes pratiques ITIL.

Notre objectif à court terme est de proposer des solutions « clés en mains » adaptées aux besoins de l'entreprise, faciles et rapides à mettre en œuvre, afin de garantir une sécurisation de leur production.

Notre objectif à moyen et long terme est d'obtenir un contrat d'infogérance au niveau de la gestion du parc et des incidents.

Nos principaux atouts par rapport à la concurrence seront notre disponibilité et notre rapidité d'intervention. Notre démarche qualité proactive sera également un de nos arguments forts.

Notre expérience dans la gestion externalisée du système d'information des entreprises apportera une garantie supplémentaire à AutoConcept dans son choix.

Enfin, notre faculté à convaincre l'entreprise et à négocier au mieux un contrat portant sur des objectifs réalistes et réalisables sera l'étape déterminante dans l'obtention de ce dernier.

Sources :

- https://fr.wikipedia.org/wiki/ISO/CEI_27002
- https://www.olfeo.com/
- https://www.legifrance.gouv.fr/
- http://www.ssi.gouv.fr/
- https://www.cnil.fr/professionnel
- https://www.axelos.com/best-practice-solutions/itil
- https://www.synology.com/fr-fr
- https://www.qnap.com/fr-fr/
- http://www.itilfrance.com/
- https://www.hadopi.fr/

Index des annexes

La CNIL accompagne les professionnels dans leur mise en conformité et aide les particuliers à maîtriser leurs données personnelles et exercer leurs droits. Elle analyse l'impact des innovations technologiques et des usages émergents sur la vie privée et les libertés.
Enfin, elle travaille en étroite collaboration avec ses homologues européens et internationaux pour élaborer une régulation harmonisée .

4 missions principales :

1. Informer / protéger

La CNIL informe les particuliers et les professionnels et répond à leurs demandes. Elle met à leur disposition des outils pratiques et pédagogiques et intervient très régulièrement pour animer des actions de formation et de sensibilisation, notamment dans le cadre de l' éducation au numérique .
Toute personne peut s'adresser à la CNIL en cas de difficulté dans l'exercice de ses droits.

Elle a pour mission de promouvoir l'utilisation des technologies protectrices de la vie privée, notamment les technologies de chiffrement des données.

2. Accompagner /conseiller

La régulation des données personnelles passe par différents instruments qui poursuivent tous un objectif de mise en conformité des organismes : avis sur des projets de loi ou de décret, autorisation pour les traitements les plus sensibles, recommandations fixant une doctrine, cadres juridiques simplifiant les formalités préalables, réponse à des demandes de conseils. La CNIL propose également une boîte à outils aux organismes qui souhaitent aller plus loin dans leur démarche de conformité: correspondants infonnatique et libertés (CIL), labels, packs de conformité (référentiels sectoriels), BCR (Binding Corporate Rules) qui encadrent les transferts de multinationales hors de l'Union Européenne.

Elle certifie la conformité des processus d'anonymisation des données personnelles dans la perspective de leur mise en ligne et de leur réutilisation.

3. Contrôler et sanctionner

Le contrôle sur place, sur pièces, sur audition ou en ligne permet à la CNIL de vérifier la mise en œuvre concrète de la loi.

Un programme des contrôles est élaboré en fonction des thèmes d'actualité, des grandes problématiques identifiées et des plaintes dont la CNIL

est saisie. La CNIL est compétente pour contrôler les systèmes de vidéoprotection autorisés par les préfectures.

Lors d'un contrôle sur place, la CNIL peut:

- accéder à tous les locaux professionnels,
- demander communication de tout document nécessaire et d'en prendre copie ,
- recueillir tout renseignement utile et entendre toute personne,
- accéder aux programmes informatiques et aux données.

A l'issue des contr ôles, la Présidente de la CNIL peut décider des mises en demeure. La formation restreinte de la CNIL, composée de 5 membres et d'un Président distinct du Président de la CNIL, peut prononcer diverses sanctions à l'issue d'une procédure contradictoire : une sanction pécuniaire (sauf pour les traitements de l'État) d'un montant maximal de 3 millions d' euros. Cette sanction peut être rendue publique ; la formation restreinte peut également ordonner l'insertion de sa décision dans la presse, ou ordonner que les organismes sanctionnés informent individuellement les personnes concernées aux frais de l'organisme sanctionné.

Le montant des amendes est perçu par le Trésor Public et non par la CNIL. La formation restreinte de la CNIL peut également prononcer :

- Une injonction de cesser le traitement.
- Un retrait de l'autorisation accordée par la CNIL.

En cas d' atteinte grave et immédiate aux droits et libertés , le président de la CNIL peut demander , par référé, à la juridiction compétente , d' ordonner toute mesure nécessaire. li peut également dénoncer au Procureur de la République les infractions à la législation dont il a connaissance.

4. Anticiper

Dans le cadre de son activité d' innovation et de prospective, la CNIL met en place une veille pour détecter et analyser les technologies ou les nouveaux usages pouvant avoir des impacts importants sur la vie privée. Elle dispose d'un laboratoire lui permettant d'expérimenter des produits ou applications innovants. Elle contribue au développement de solutions technologiques protectrices de la vie privée en conseillant les entreprises le plus en amont possible, dans une logique de privacy by design. Pour renforcer sa réflexion, elle a créé un comité de la prospective faisant appel à des experts extérieurs qui la conseille pour élaborer un programme annuel d'études et d' explorations.

Elle a pour mission de conduire une réflexion sur les problèmes éthiques et les questions de société soulevés par l'évolution des technologies numériques.

LES MOTS DE PASSE N'ONT PLUS DE SECRET POUR VOUS!

****

UN MOT DE PASSE EN BÊTON |

Un bon mot de passe doit contenir 12 caractères, d'au moins 4 types différents : des minuscules, des majuscules, des chiffres et des caractères spéciaux. Il peut être plus court si votre compte est équipé de sécurités complémentaires !

****

IL NE DIT RIEN SUR VOUS |

Personne ne doit deviner votre mot de passe à partir du nom de votre chien ou de votre film préféré. Idem pour le code de votre smartphone : préférez un nombre aléatoire à une année.

****

UN COMPTE, UN MOT DE PASSE |

Pour éviter les piratages en cascade, chacun de vos comptes en ligne qui présente un caractère sensible (banque, messagerie, réseau social, etc.) doit être verrouillé avec un mot de passe propre et unique.

****

NE JAMAIS L'ABANDONNER EN PLEINE NATURE |

Les post-it, les fichiers texte, votre smartphone ou votre boîte de messagerie ne sont pas conçus pour sécuriser le stockage de vos mots de passe. Pensez aussi à ne jamais les enregistrer dans le navigateur d'un ordinateur partagé.

****

DEUX CADENAS VALENT MIEUX QU'UN |

Quand le service vous le propose, activez la double authentification. Si quelqu'un se connecte à votre compte depuis un terminal inconnu, le site vous prévient par SMS/e-mail. Libre à vous d'autoriser ou de refuser l'accès !

****

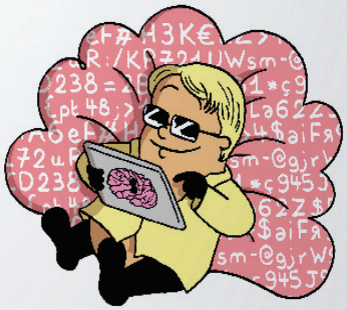
LES RETENIR SANS LES ÉCRIRE

... EN TRAVAILLANT VOS NEURONES |

Mémorisez une phrase puis utilisez la première lettre de chaque mot pour créer votre mot de passe. La phrase doit contenir des chiffres et des caractères spéciaux !

... EN REPOSANT VOS MÉNINGES |

Utilisez un gestionnaire de mots de passe ou un trousseau d'accès chiffré pour stocker vos mots de passe en toute sécurité. Vous n'aurez à retenir qu'un mot de passe pour accéder à l'ensemble de vos comptes !



****

PLUS DE CONSEILS SUR WWW.CNIL.FR

CNIL.
COMMISSION NATIONALE INFORMATIQUE & LIBERTÉS

Illustrations : Martin Vidberg

Annexe 3

Dix règles de base de l'ANSSI

Voici les dix règles de base, en quelque sorte les 10 commandements de la sécurité sur l'Internet.

1. Utiliser des mots de passe de qualité. Le dictionnaire définit un mot de passe « comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé ». Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficile à retrouver à l'aide d'outils automatisés, et difficile à deviner par une tierce personne.
2. Avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu personnel, etc. La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des logiciels). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.
3. Effectuer des sauvegardes régulières. Un des premiers principes de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de ses données est une condition de la continuité de votre activité.
4. Désactiver par défaut les composants ActiveX et JavaScript. Les composants ActiveX ou JavaScript permettent des fonctionnalités intéressantes, mais ils présentent aussi des risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. En dépit de la gêne que cela peut occasionner, il est conseillé de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si l'on estime être sur un site de confiance.
5. Ne pas cliquer trop vite sur des liens. Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.
6. Ne jamais utiliser un compte administrateur pour naviguer. L'utilisateur d'un ordinateur dispose de privilèges ou de droits sur celui-ci. Ces droits permettent ou non de conduire certaines actions et d'accéder à certains fichiers d'un ordinateur. On distingue généralement les droits dits d'administrateur et les droits dits de simple utilisateur. Dans la majorité des cas, les droits d'un simple utilisateur sont suffisants pour envoyer des messages ou surfer sur l'Internet. En limitant les droits d'un utilisateur, on limite aussi les risques d'infection ou de compromission de l'ordinateur.
7. Contrôler la diffusion d'informations personnelles. L'Internet n'est pas le lieu de l'anonymat et les informations que l'on y laisse échappent instantanément ! Dans ce contexte, une bonne pratique consiste à ne jamais laisser de données personnelles dans des forums, à ne jamais saisir de coordonnées personnelles et sensibles (comme des coordonnées bancaires) sur des sites qui n'offrent pas toutes les garanties requises. Dans le doute, mieux vaut s'abstenir…
8. Ne jamais relayer des canulars. Ne jamais relayer des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc. Quel que soit l'expéditeur, rediffuser ces messages risque d'induire des confusions et de saturer les réseaux.
9. Soyez prudent : l'Internet est une rue peuplée d'inconnus ! Il faut rester vigilant ! Si par exemple un correspondant bien connu et avec qui l'on échange régulièrement du courrier en français, fait parvenir un message avec un titre en anglais (ou toute autre langue) il convient de ne pas l'ouvrir. En cas de doute, il est toujours possible de confirmer le message en téléphonant. D'une façon générale, il ne faut pas faire confiance machinalement au nom de l'expéditeur qui apparaît dans le message et ne jamais répondre à un inconnu sans un minimum de précaution.
10. Soyez vigilant avant d'ouvrir des pièces jointes à un courriel : elles colportent souvent des codes malveillants. Une des méthodes les plus efficaces pour diffuser des codes malveillants est d'utiliser des fichiers joints aux courriels. Pour se protéger, ne jamais ouvrir les pièces jointes dont les extensions sont les suivantes : .pif (comme une pièce jointe appelée photos.pif) ; .com ; .bat ; .exe ; .vbs ; .lnk. À l'inverse, quand vous envoyez des fichiers en pièces jointes à des courriels privilégiez l'envoi de pièces jointes au format le plus « inerte » possible, comme RTF ou PDF par exemple. Cela limite les risques de fuites d'informations.

Annexe 4

Modèle d'une charte informatique :

1. Le rappel des règles de protection des données et les sanctions encourues en cas de non respect de la loi.
2. Le champ d'application de la charte, qui inclut notamment :
   - les modalités d'intervention du service de l'informatique interne ;
   - les moyens d'authentification ;
   - les règles de sécurité auxquelles se conformer, ce qui peut inclure par exemple de :
     - signaler au service informatique interne toute violation ou tentative de violation suspectée de son compte informatique et de manière générale tout dysfonctionnement ;
     - ne jamais confier son identifiant/mot de passe à un tiers ;
     - ne pas modifier les paramétrages du poste de travail ;
     - ne pas installer, copier, modifier, détruire des logiciels sans autorisation ;
     - verrouiller son ordinateur dès que l'on quitte son poste de travail ;
     - ne pas accéder, tenter d'accéder, ou supprimer des informations qui ne relèvent pas des tâches incombant à l'utilisateur ;
     - définir les modalités de copie de données sur un support externe, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant des règles préalablement définies.
3. Les modalités d'utilisation des moyens informatiques et de télécommunications mis à disposition comme :
   - le poste de travail ;
   - les équipements nomades ;
   - l'espace de stockage individuel ;
   - le réseau local ;
   - internet ;
   - la messagerie électronique ;
   - le téléphone.
4. Les conditions d'administration du système d'information, et l'existence, le cas échéant, de:
   - systèmes automatiques de filtrage ;
   - systèmes automatiques de traçabilité ;
   - gestion du poste de travail.
5. Les responsabilités et sanctions encourues en cas de non respect de la charte.

IDK

Annexe 5

Evaluez le niveau de sécurité des données personnelles dans votre organisme

Avez-vous pensé à ?

Fiche		Mesure	
1	Analyser les risques	**Recensez** les fichiers et données à caractère personnel et les traitements	❑
		Déterminez les menaces et leurs impacts sur la vie privée des personnes	❑
		Mettez en œuvre des **mesures de sécurité adaptées** aux menaces	❑
2	Authentifier les utilisateurs	Définissez un identifiant ***(login)*** unique à chaque utilisateur	❑
		Adoptez une **politique de mot de passe utilisateur rigoureuse**	❑
		Obligez l'utilisateur à **changer son mot de passe après réinitialisation**	❑
3	Gérer les habilitations & sensibiliser les utilisateurs	**Définissez des profils d'habilitation**	❑
		Supprimez les permissions d'accès obsolètes	❑
		Documentez les procédures d'exploitation	❑
		Rédigez une **charte informatique** et annexez-la au **règlement intérieur**	❑
4	Sécuriser les postes de travail	**Limitez le nombre de tentatives d'accès** à un compte	❑
		Installez un «**pare-feu**» *(firewall)* logiciel	❑
		Utilisez des **antivirus régulièrement mis à jour**	❑
		Prévoyez une procédure de **verrouillage automatique de session**	❑
5	Sécuriser l'informatique mobile	Prévoyez des **moyens de chiffrement** pour les **ordinateurs portables** et les unités de stockage amovibles (**clés USB**, CD, DVD…)	❑
6	Sauvegarder et prévoir la continuité d'activité	Effectuez des **sauvegardes régulières**	❑
		Stockez les supports de sauvegarde dans un endroit sûr	❑
		Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	❑
		Prévoyez et testez régulièrement la **continuité d'activité**	❑
7	Encadrer la maintenance	**Enregistrez les interventions** de maintenance dans une **main courante**	❑
		Effacez les données de tout matériel avant sa **mise au rebut**	❑
		Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	❑
8	Tracer les accès et gérer les incidents	Prévoyez un **système de journalisation**	❑
		Informez les utilisateurs de la mise en place du système de journalisation	❑
		Protégez les équipements de journalisation et les informations journalisées	❑
		Notifiez les personnes concernées des accès frauduleux à leurs données	❑
9	Protéger les locaux	**Restreignez les accès** aux locaux au moyen de **portes verrouillées**	❑
		Installez des **alarmes anti-intrusion** et vérifiez-les périodiquement	❑
10	Protéger le réseau informatique interne	**Limitez les flux réseau au strict nécessaire**	❑
		Sécurisez les accès distants des appareils informatiques nomades par **VPN**	❑
		Utilisez le protocole SSL avec une clé de 128 bits pour les **services web**	❑
		Mettez en œuvre le protocole WPA - AES/CCMP pour les réseaux WiFi	❑
11	Sécuriser les serveurs et les applications	Adoptez une **politique de mot de passe administrateur rigoureuse**	❑
		Installez sans délai les **mises à jour critiques**	❑
		Assurez une **disponibilité** des données	❑
12	Gérer la sous-traitance	Prévoyez une **clause spécifique** dans les contrats des sous-traitants	❑
		Assurez-vous de l'**effectivité des garanties** prévues (audits de sécurité, visites...)	❑
		Prévoyez les **conditions de restitution** et de destruction des données	❑
13	Archiver	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	❑
		Détruisez les archives obsolètes de manière sécurisée	❑
14	Sécuriser les échanges avec d'autres organismes	**Chiffrez** les données avant leur envoi	❑
		Assurez-vous qu'il s'agit du **bon destinataire**	❑
		Transmettez le **secret** lors d'un envoi distinct et via un canal différent	❑