TRIOUX Jimmy
SIO1

TP - La charte informatique

Les points clés de la charte informatique

Cette charte informatique datant de 2012 présente certains points clés concernant le télétravail.

1. Cadre du télétravail :

Le télétravail est défini comme étant un engagement mutuel entre l'agent et sa hiérarchie. C'est une démarche volontaire et réversible et ne peut en aucun cas être imposé à l'agent.

2. Modalités de mise en œuvre :

Celle-ci spécifie notamment le respect de la vie privée par le biais de plages horaires définies, de l'organisation du travail par l'agent et de lui fixer des objectifs plutôt qu'imposé des horaires.

Les points clés de la charte informatique

3. Moyens mis à disposition

Les ressources sont fournies par le Conseil régional (logiciels, ordinateurs), une assistance informatique est disponible pour les télétravailleurs pendant les heures ouvrées de bureau, des règles liés à **l'utilisation et l'installation des logiciels** et l'obligation de respecter les règles concernant la **confidentialité**, **la protection des données et de sécurité**.

4. Exercice du télétravail

Le télétravailleur doit **prévoir un espace de travail à son domicile** et doit être régulièrement **évaluer par le biais d'un bilan par la MPPAC**.

Mise à jour de la politique des données avec le RGPD

Cette charte informatique (relative au télétravail) a été rédigée en 2012 alors que le règlement général sur la protection des données (**RGPD**) est entré en vigueur en 2018. Désormais, la loi impose de nouvelles règles que nous devons appliquer rendant obsolète certains points clés de la charte et d'autres à ajouter.

1. **Cadre du télétravail :**
   Dans le cadre juridique, préciser la formation obligatoire sur le traitement des données dans le cadre du télétravail pour les agents.

2. **Modalités de mise en œuvre**
   Respect de la vie privée
   - Ajouter des clauses pour prévenir de la collecte abusive sur le stockage des données personnelles des agents.
   - Mentionner explicitement l'interdiction d'utiliser des outils de surveillance.
   - Limiter la collecte des données à ce qui est nécessaire pour l'activité de l'agent.

3. **Moyens mis à disposition et traitement de l'information**
   Equipements de travail
   - Garantir la configuration des équipements pour minimiser les risques d'accès non autorisé (contrôle des accès, chiffrement…)
   - Mentionner que l'équipement est sous contrôle du Conseil régional.

Mise à jour de la politique des données avec le RGPD

Installation et utilisation de logiciels
- Interdire tous les logiciels/applications pouvant compromettre la sécurité des données
- Audits permettant de vérifier les logiciels installés par rapport à la conformité du RGPD.

Confidentialités et protection des données, sécurité des systèmes d'information
- Offrir des solutions de sensibilisation aux télétravailleurs par rapport aux bonnes pratiques (mots de passe, réseaux publics, usage de VPN, BitLocker etc…)
- Instaurer une politique de gestion des incidents (délais de notifications à la CNIL, plans d'actions)

4. Exercice du travail

Evaluation

- Intégrer des critères pour l'évaluation des bonnes pratiques concernant les télétravailleurs.
- Réaliser des audits par rapport aux données manipulées par les télétravailleurs.

Les usages personnels :

Il est impératif de savoir limiter l'usage des appareils en fonction du cadre.

Dans un contexte d'usage personnel, le service informatique doit impérativement rappeler que l'utilisation des équipements fournies par l'entreprise doivent être utilisé uniquement dans le cadre professionnel.

De plus, il est important de rappeler dans la charte que l'installation de logiciels ou de leur utilisation à des fins personnelles est strictement interdite.

Les usages professionnels :

Dans un cadre d'usage professionnel, les équipements doivent être utilisés uniquement pour les tâches liées au télétravail.

Les agents devront se connecter au système d'information avec des solutions de sécurisation comme un VPN (**Cisco Secure Client**) ou une connexion chiffrée.

Appliquer des règles de confidentialité et de protection des données à tous les fichiers et documents manipulés.

La politique concernant les fichiers en provenance d'internet

Bien que la région traite de l'installation des logiciels ainsi que de leur utilisation dans le point **3-2** et **3-4**, elle ne traite pas précisément la provenance des fichiers sur internet.

En effet, la charte informatique mentionne **l'interdiction aux utilisateurs d'utilisés des logiciels non autorisés** par le service informatique. Hors, il serait préférable de **créer des droits d'utilisateurs** afin de restreindre l'accessibilité à des logiciels non nécessaires à l'exercice du travail des collaborateurs afin d'éviter aux salariés de **télécharger des fichiers pouvant être malveillants** (virus, phishing, ingénierie sociale, fuite de données, intégrité du système…).

Il est également nécessaire de **mettre en place des formations**, dans le but de, sensibiliser les utilisateurs aux **bonnes pratiques** (vérifier les extensions de fichier, ouvrir les fichiers non modifiables, c'est-à-dire, sans exécution de script comme des fichiers PDF).

La politique concernant les fichiers en provenance d'internet

De plus, nous n'avons pas de mention concernant les outils de sécurisation alors il faudra instaurer obligatoirement l'installation et la configuration d'un antivirus pour les télétravailleurs.

Également encouragé la pratique du sandboxing où l'intérêt est d'ouvrir les fichiers dans un environnement isolé.

Le service informatique devra également bloquer au préalable pour les télétravailleurs certains types de fichiers comme les **.exe** (fichier exécutable), **.docx/.xls** qui peuvent contenir des macros s'exécutant en fond sans que l'utilisateur puisse le remarquer.

Instaurer un chiffrement obligatoire pour tous les fichiers qui circule dans l'environnement de travail.

Le service informatique devra mettre en place des audits afin de vérifier si les télétravailleurs respectent les règles.

Comment diffuser l’information aux utilisateurs ?

- En favorisant les échanges entre collaborateurs.
- Utiliser un logiciel de communication qui centralise tous les employés (Microsoft Teams par exemple) afin de notifier régulièrement des comportements à adopter.
- Mettre des affiches dans les bureaux, via des emails.
- Organiser des sessions/visioconférences ayant pour but de former les agents.
- Distribuer la charte informatique à chaque salarié de l’entreprise et également créer un guide des bonnes pratiques pour l’utilisateur
- Mettre en place des outils interactifs comme des quiz ou des questionnaires sur la cybersécurité.