certains cas, les agents peuvent utiliser leurs matériels personnels pour exercer leur activité en télétravail. Cela s'appelle le BYOD ("Bring Your Own Device").
Dans tous les cas, ces équipements doivent être protégés car le risque de perte ou vol de matériel, la compromission du matériel ou des informations contenues dans le matériel. L'accès à des données confidentiel est très probable. Il faut donc sensibiliser les agents aux bonnes pratiques en matière de sécurité. Il faut également maîtriser la gestion des utilisateurs nomades et des applications utilisées.
Par le BYOD, il faut engager des actions spécifique. En effet la collectivité ne maîtrise pas les logiciels installés, la version des navigateurs, l'équipement d'anti-virus.
Par exemple, créer une bulle de sécurité permettant de cloisonner les parties de l'outil personnel et l'usage professionnel. ou encore exiger le verrouillage du terminal, par un mot de passe et l'installation d'un logiciel d'antivirus à jour.

Propositions opérationnelles.

I Méthodologie projet et analyse du besoin.

1. Définition d'un groupe de travail.

Afin d'intégrer tous les services de la collectivité, un groupe de travail devra être mis en place. Le groupe sera composé d'élus ainsi que de cadres ou directeurs de chaque services.
Nous pourrons identifier les besoins en terme de télétravail de chaque service de la collectivité et identifier la liste des utilisateurs susceptibles de faire du télétravail.
Ce groupe de travail se réunira régulièrement.
Un compte rendu sera envoyé aux élus et aux agents de la collectivité si besoin.

FONCTION PUBLIQUE TERRITORIALE
INTERREGION EST

Intitulé du concours ou de l'examen : Technicien principal 2cl

CONCOURS [X] (1) — Interne [ ] (1) — Externe [X] (1)
EXAMEN [ ] (1) — Troisième concours [ ] (1)
(1) Cocher la case correspondante

ouvert le 15 Avril 2021
à Vandoeuvre-lès-Nancy
Epreuve de Rapport technique.
Spécialité et/ou option : Ingénierie Informatique et Systèmes d'information.
(le cas échéant uniquement)

Numéro d'anonymat
Cadre réservé à l'administration
8702861760

PARTIE A LAISSER EN BLANC ET A RABATTRE

Humecter, rabattre et coller la partie gommée.
OBLIGATOIRE POUR GARANTIR VOTRE ANONYMAT

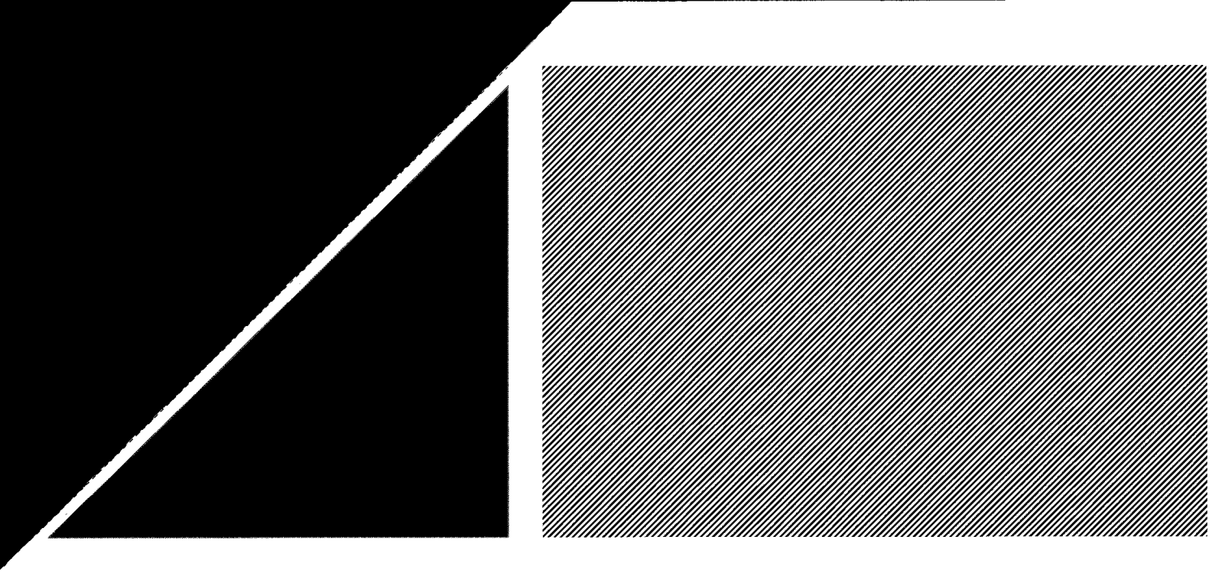
Ville de Techniville.

le 15 Avril 2021,

Rapport technique.
A l'attention du directeur des systèmes d'information.

Objet : Le télétravail et la sécurité informatique.

En mars 2018, 4,65% des agents territoriaux étaient en télétravail contre 2,5% pour l'administration centrale.
Ce chiffre est en augmentation, en effet, en France, les employés et leurs employeurs accordent de plus en plus d'importance pour le télétravail. La diminution du temps de transport, une confiance plus accrue permettraient aux employés d'atteindre un certain bien-être au travail et donc d'augmenter leur productivité. Néanmoins, l'accès aux données et l'utilisation des équipements de la collectivité en dehors des locaux professionnels entraînent un risque en matière de sécurité pour l'entreprise.
Dans un premier temps nous allons rappeler le cadre réglementaire défini pour l'exercice du télétravail puis définir les enjeux en matière de sécurité informatique ainsi que la stratégie à mettre en place.



I Le cadre réglementaire du télétravail.

1. Les lois et décrets réglementaire.

C'est la loi n°2012-347 du 12 mars 2012 ainsi que le décret 2016-151 du 11 février 2016 qui définissent la possibilité pour les agents publics d'exercer leurs fonctions en télétravail.
Ces lois sont aussi complétées par des arrêtés ministériels comme par exemple l'instruction du 11 août 2016 du ministère de l'Agriculture sur les modalités pratiques de mise en oeuvre du télétravail.
L'ordonnance dite "Macron" entrée en vigueur le 22 septembre 2017, a assoupli les conditions permettant de recourir au télétravail.
Aussi, il ne faut pas oublier que la mise en place du télétravail doit être compatible avec le règlement général de protection des données qui est entré en vigueur le 25 mai 2018.

2. Les conditions du télétravail.

Ces lois et décrets visent à encadrer les conditions matériels, le lieu d'exercice du télétravail.
En effet le lieu d'exercice doit être conforme et répondre à plusieurs exigences pour être compatible avec le télétravail. (conformité de l'installation électrique, connexion haut débit, ergonomie

etc...).
Les règles de gestion doivent être définies par la collectivité.
Concernant la prise en charge des coûts liés au télétravail le décret indique que l'employeur prend en charge les coûts découlant directement de l'exercice des fonctions en télétravail.

II Les enjeux en matière de sécurité informatique et la définition d'une stratégie informatique.

L'utilisation des données et des équipements informatique de la collectivité en dehors de notre réseaux et de nos locaux augmente le risque de perte de données et d'attaques il faut donc mettre en place une stratégie

1. Choix d'une architecture pour sécuriser les données.

Afin de sécuriser les données accessibles en mode nomadisme il convient de mettre en place une architecture technique adaptée et sécurisée. Plusieurs choix sont possibles, mais bien sûr il faut que la solution puisse crypter et rendre illisible les données en cas de pertes ou de vol.
Une première solution est d'utiliser les solutions en mode Cloud. le Cloud propose des performances intéressantes en terme de sécurité. Les fournisseurs fournissent des infra-structures performantes, testées ainsi que des moyens humains que certaines collectivités ne disposent pas. Les solutions gèrent les habilitations en fonction du type d'utilisateur en temps réel et ont une forte réactivité en cas de fuite de données.
La mise en place d'un VPN permet aux agents d'accéder au réseau local de la collectivité à distance. Il faut donc que la connexion internet soit sécurisée.
Afin de sécuriser au mieux les données, il conviendrait d'utiliser un logiciel de DLP qui permettrait de définir les données par utilisateur et générerait des alertes et des actions protectrices pour empêcher toutes actions frauduleuses

2. Sécuriser les équipements.

Dans le cadre du télétravail, la majorité des structures équipent leurs agents de matériels informatiques mais dans

ALDOM [002] - 03 85 78 99 11 - RÉF. 20796

FONCTION PUBLIQUE TERRITORIALE
INTERREGION EST

Intitulé du concours ou de l'examen : Technicien principal 2 Cl

CONCOURS [X] (1) — Interne [ ] (1) — Externe [X] (1)

EXAMEN [ ] (1) — Troisième concours [ ] (1)

(1) Cocher la case correspondante

ouvert le 15 Avril 2021

à Vandoeuvre-lès-Nancy

Epreuve de Rapport technique.

Spécialité et/ou option : Ingénierie Informatique et Systèmes d'information
(le cas échéant uniquement)

Numéro d'anonymat
Cadre réservé à l'administration

8702861760

PARTIE A LAISSER EN BLANC ET A RABATTRE

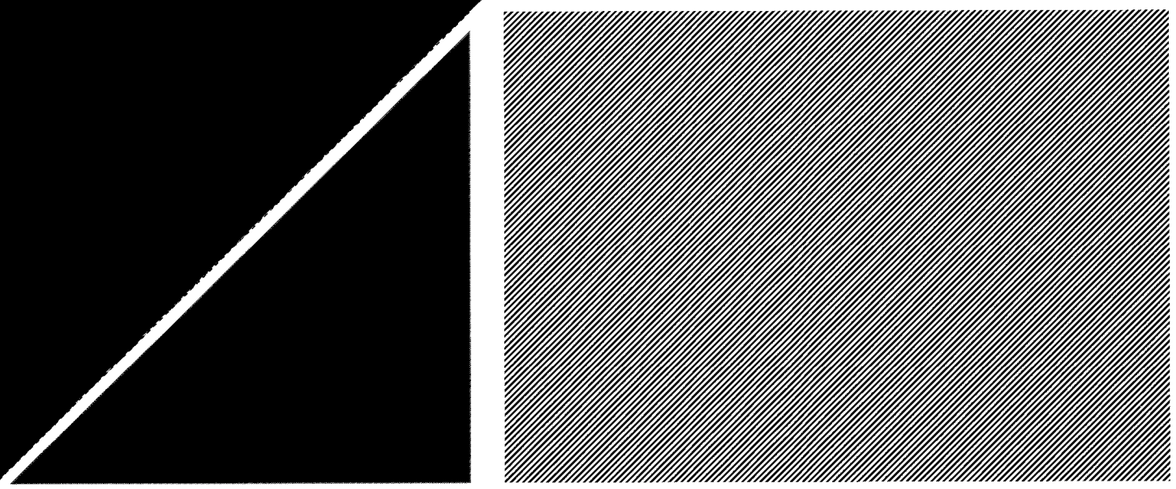
Humecter, rabattre et coller la partie gommée.
OBLIGATOIRE POUR GARANTIR VOTRE ANONYMAT

2. Identifier les utilisateurs et les activités:
Chaque service de la collectivité devra nous fournir la liste des utilisateurs qui pourraient exercer leurs activités en télétravail.
Chaque utilisateur devra preciser sa fonction, ses missions, les applications utilisées (et leur mode d'accès), la sensibilité des données liées à l'activité)

3. Etat des lieux de la sécurité informatique
Un audit de sécurité va être commandé auprès d'une société spécialisée. Cet audit nous permettra d'avoir un état de la sécurité informatique de la collectivité et cette analyse nous permettra de savoir quelles sont les solutions à privilégier.

II. Les actions à mener et les différents enjeux

1. Enjeux financier.
Nous devons évaluer le nombre d'ordinateurs nécessaires ainsi, une réunion avec le service juridique et finance doit être organisée afin de savoir si le marché actuel nous permettra de racheter une flotte d'ordinateur.



2. Les moyens humains

L'acquisition de nouveaux matériels nécessitera le paramétrage de ceux-ci et l'installation de nouveaux logiciels spécifiques aux télétravail. Nous devons donc refaire un point sur la charge de travail des équipes du service informatique.

3. Les solutions techniques

Il faudra que nous mettions en place de nouvelles solutions de virtualisation permettant aux agents de se connecter au réseau de la collectivité en toute sécurité. La mise en place du MDM de la collectivité devra être réalisé et reparamétré.

De plus il faudra vérifier que les applications suivantes fonctionnent correctement

- le webmail de la collectivité.
- l'accès à la messagerie instantanée.
- le logiciel de softphone.

4. La formation et la sensibilisation des données.

En partenariat avec le service des ressources humaines des sessions de formation devront être organisées.

Ces formations devront faire comprendre aux employés les risques et les conséquences potentielles de la perte d'un appareil ou de la perte de données confidentielle.

Des formations sur l'ergonomie et les bonne pratiques en télétravail devront être organisées.

Ces formations permettront aussi de sensibiliser les agents à la sécurité informatique (utilisation de clé USB, dossier papier).

Cette campagne de sensibilisation sera réalisée avec le service communication via l'intranet de la collectivité et la mise en place de panneau d'affichage en interne.

Conclusion.

L'intérêt de la collectivité pour le télétravail et la sécurité est un véritable enjeu pour l'avenir. Il conviendra par la suite d'évaluer les solutions mises en place via des indicateurs qui seront définis par notre groupe de travail et des sondages auprès des agents.