POD MAATSCHAPPELIJKE INTEGRATIE
BETER SAMEN LEVEN
SPP INTÉGRATION SOCIALE
MIEUX VIVRE ENSEMBLE

Madame,
Monsieur,

La crise du coronavirus a incité les autorités responsables à demander à travailler autant que possible à domicile afin de lutter contre la propagation du virus COVID-19. De nombreux employés de CPAS travaillent désormais (en tout ou en partie) à domicile. Ceci est bien sûr approprié pour permettre aux CPAS de continuer à fonctionner.

L'objectif en premier lieu est bien entendu d'aider au mieux les demandeurs. Cela doit être la priorité, surtout dans les circonstances difficiles que nous vivons.

Par ailleurs, nous sommes bien conscients que les autorités locales et les CPAS ont dû réagir très rapidement et passer très rapidement au télétravail.

Si les travailleurs sociaux ou autres employés utilisant des données personnelles doivent travailler à domicile, les mesures de sécurité nécessaires doivent être prises. Pensez par exemple, si possible, à travailler dans une pièce séparée de celle où les autres membres de la famille sont présents, à éteindre votre ordinateur ou activez l'économiseur d'écran si vous ne travaillez pas sur votre ordinateur, etc. (voir également ci-dessous)

Le code déontologique des travailleurs sociaux reste bien entendu d'application.

Malgré ces circonstances difficiles, il reste important de rechercher une cybersécurité maximale.

Ainsi les mesures de sécurité de la BCSS s'appliquent (encore toujours) lors de la consultation des flux de la BCSS et pour les institutions utilisant des lecteurs de cartes d'identité.

Nous rappelons encore ici ces mesures:

1. Le personnel continue à travailler physiquement dans les locaux du CPAS : il n'y a alors pas de problème de sécurité, ce périmètre est censé être suffisamment sécurisé et conforme aux normes minimales de la BCSS ;
2. Les employés ont un PC (ordinateur de bureau ou ordinateur portable) de leur employeur : cet ordinateur portable doit être configuré normalement et conformément aux normes minimales de sécurité du KSZ (voir annexe 1 à la fin du document).
3. Les employés ont un PC privé et veulent travailler avec celui-ci depuis leur domicile : pour des raisons de sécurité, cette solution n'est autorisée que sous certaines conditions strictes (voir vulnérabilités en annexe 2), sauf en cas de travail avec une solution de type bureau virtuel (par exemple Citrix, Awingu, BeSecure...) installée. Si vous souhaitez travailler à partir d'un PC privé, sans technologie de bureau virtuel, les critères suivants doivent être remplis:

a. Le mot de passe doit contenir 12 caractères, y compris des majuscules, des minuscules, des chiffres et un caractère spécial. De plus, une authentification à deux facteurs doit être utilisée (https://www.safeonweb.be/fr/utilisez-des-mots-de-passe-surs);

b. Pendant le travail, aucune autre recherche ne peut être effectuée sur Internet via le navigateur ;

c. A la fin de la session de travail / consultation /…ou pendant la pause, celle-ci doit être clôturée ,

d. Personne d'autre que l'employé n'est autorisé à voir le contenu des sessions ;

e. Le pare-feu du CPAS doit être configuré avec le maximum de restrictions possibles. Par exemple, limiter la région depuis laquelle les accès extérieurs sont autorisés, limiter aussi le temps d'ouverture de la connexion (exemple : pendant les heures de travail et pas le week-end…).

Risque : s'il y a trop de connexions à distance, cela peut saturer la largeur de bande (le réseau). Cela signifie que les agents risquent d'avoir des connexions très lentes.

Qui peut vous aider ?

Compte tenu des contraintes citées ci-dessus :

- l'informaticien du CPAS ou de la commune ou votre fournisseur informatique peut vous aider à effectuer les diverses phases de sécurité nécessaires au télétravail soit :
    - en installant un outil de prise de contrôle professionnel à distance de votre ordinateur comme par exemple : connexion VPN + utilisation de l'outil "accès bureau à distance" (**uniquement** pour l'installation ou le dépannage et cet outil sera ensuite fermé);
    - en vous préparant un PC fixe du CPAS qu'il mettra à votre disposition pour l'installer chez vous et travailler plus facilement, auquel cas le PC sera utilisé **uniquement** pour le CPAS ;
    - en préparant un PC portable et en le mettant à votre disposition ;
    - en préparant un client léger (ou via Citrix) si le CPAS travaille avec cette technologie ;
    - en vous faisant télécharger une exécutable spécifique qui s'installera automatiquement dans le cas de la licence terminal – serveur.

- A noter que les utilisateurs qui font du télétravail ne laisseront jamais leur écran ouvert mais qu'ils activeront le verrouillage dès qu'ils s'absentent, ceci afin de garantir la confidentialité et protéger les données à caractère personnel. Cette précaution est applicable aussi bien pour les applications connectées à la BCSS que pour tout autre traitement de dossier écrit ou oral (téléphone, conférence téléphonique ou téléconférence, chat, vidéo, etc.).

- Par principe, il est demandé de ne rien imprimer chez soi mais si cela s'avère indispensable, le document imprimé sera rangé dans un endroit sécurisé et uniquement accessible à l'agent responsable. Le document sera amené au CPAS ou délivré à qui de droit dès que possible ou détruit.

- Attention, pour les AS ou autres agents qui doivent se connecter à distance à la BCSS, les outils suivants sont obligatoires sous peine de blocage technique :
    - Passer par un VPN et Explore ou Publiwin;
    - Disposer d'un lecteur de carte d'identité électronique pour vous identifier sur le portail de la sécurité sociale, lecteur indépendant ou intégré dans le clavier (la meilleure solution).

- Disposer d'une police d'utilisation rédigée par votre DPD et/ou votre juriste qui inclura une clause de confidentialité comprenant les contraintes suivantes :
  - pas d'accès volontaire ou non à toute personne étrangère au CPAS à votre session sur votre PC;
  - pas d'accès volontaire ou involontaire à toute personne étrangère au CPAS à votre PC portable appartenant au CPAS ;
  - pas de communication des mots de passe (il va de soi que votre informaticien a les droits d'administrateur) ;
  - pas de consultation de sites internet à des fins personnelles en même temps que votre session VPN avec le CPAS (fermer la session VPN et ouvrir celle du navigateur si cela s'avère nécessaire) .

Proximus, Publiwin (entre autres) offrent des solutions fiables de VPN avec RDP (remote deskstop protocol) depuis le PC portable ou non et des licences de RDC (Remote Deskstop Connection) de Microsoft (licence terminal server CAL user).

Il va de soi que votre informaticien ou votre fournisseur informatique pourra, également, vous aider. Faites cependant attention au fait que cela ne doit pas permettre à votre fournisseur d'installer plus de droits d'administration, de connexion ou d'aide en ligne que nécessaire et qui ne sont pas conformes au RGPD et aux normes de la BCSS.

Enfin, n'hésitez pas à nous contacter en cas de problème aux adresses suivantes :

gilles.kempgens@mi-is.be et à mi.dpo@mi-is.be ou au 0473.85.26.24.

Annexe 1

Rappel des mesures de sécurité à respecter sur les PC portables – laptops – deskstops :

a. le PC n'a pas de droit d'administrateur ;

b. le PC ne contient pas de données à caractère personnel mais s'il en contient, les données doivent être cryptées (Bitlocker est un outil Microsoft gratuit si vous avez une version Microsoft Business ou Entreprise) ;

c. la connexion se fait via un VPN qui se connecte depuis le PC portable au réseau du CPAS ;

d. lors de la connexion via VPN, une GPO (Group Policy Object à développer en interne ou à faire développer sur le pare-feu ou sur le Network Access Control) examinera si l'antivirus et l'OS sont à jour avant d'autoriser la connexion et si ce n'est pas le cas, la GPO forcera les mises à jour avant d'autoriser la connexion ;

e. la GPO interdira toute utilisation d'un navigateur pour aller sur internet tant que l'utilisateur est connecté au réseau du CPAS via VPN (exemples de navigateurs : Internet Explorer, Edge, Mozilla, Chrome), à noter qu'il est possible d'aller sur internet via le VPN mais ceci est conseillé uniquement pour les consultations professionnelles ;

f. les connexions se feront en remote deskstop protocol , c'est-à-dire à distance sans conserver aucune donnée mais en contenant l'ensemble des applications métier tandis que quoi la connexion se fait en direct du PC vers les serveurs et les bases de données .

Attention : en cas d'un nombre trop grand de connexions à distance, la bande passante risque d'être saturé très vite.

ANNEXE 2

LISTE DE QUELQUES VULNERABILITES LORSQUE VOUS TRAVAILLEZ DEPUIS UN PC PRIVE :

1) l'administrateur – propriétaire du PC partage son PC avec la famille ;
2) les versions Windows 7 ne sont plus fiables ;
3) il n'est pas certain qu'un vieux PC supportera bien un VPN ;
4) le respect des normes minimales impose 3 mots de passe (un mot de passe admin, un mot de passe utilisateur pour la session de l'agent et un mot de passe VPN) ;
5) le PC doit être en ordre d'antivirus et il n'est pas certain qu'il supporte le poids d'un nouvel antivirus .
6) l'utilisation d'un PC privé suppose que le propriétaire – utilisateur ferme son VPN avant d'aller sur internet pour son usage propre et inversement.