



Service Informatique
ASSURMER
2022

Date	Rédacteur	Validateur
07 septembre 2022	LE DOHER Loïc	

Table des matières

Contexte et définition du besoin :.....	2
Objectif :	2
Sécurité du SI :	3

Contexte et définition du besoin :

La volonté de l'entreprise aujourd'hui est de dématérialiser tous les processus (exemple : la création de devis, la conclusion de contrats, ...), avec la crise sanitaire et les différents problèmes que cela a causé (exemple : utilisation de matériel personnel), le télétravail est devenu indispensable.

Ainsi, pour Assurmer, il est devenu indispensable de fournir aux employés une solution de travail à distance.

Objectif :

L'objectif est de fournir à tous les employés un poste de travail mobile, c'est-à-dire un ordinateur portable pour travailler à distance et/ou se déplacer et aller à la rencontre des clients. Cela permettrait d'instaurer un climat de confiance avec les clients et de les fidéliser. Pour cela, cet ordinateur doit être rapide, efficace et avoir une bonne autonomie pour ne pas faire perdre du temps aux employés. Il faut donc avoir un bon processeur et une bonne ram.

Pour le stockage, il n'est pas nécessaire d'en avoir beaucoup puisque le collaborateur va travailler sur l'intra de l'entreprise. Il faudra tout de même une carte réseau wifi pour permet aux collaborateurs de travail partout. L'ordinateur devra être léger et avoir une petite taille pour pouvoir être facilement transportable.

Sécurité du SI :

Pour la sécurité de l'ordinateur du collaborateur, nous avons plusieurs préconisations :

Tout d'abord pour se connecter à la session et avoir une bonne sécurité, nous avons 2 choix

2FA (= authentification à double facteur): Méthode d'authentification forte par laquelle un utilisateur peut accéder à son ordinateur après avoir présenté deux preuves d'identité distinctes à un mécanisme d'authentification

Le processus d'authentification nécessite ici la combinaison d'au moins deux facteurs provenant de deux catégories différentes parmi les suivantes :

- Quelque chose que je connais (facteur de connaissance), comme un mot de passe, une phrase de passe ou un code PIN.
- Quelque chose que j'ai (facteur de possession), comme un appareil (smartphone, ordinateur, etc.), un token physique, une carte à puce.
- Quelque chose qu'ils sont (facteur d'inhérence), soit une empreinte digitale, une reconnaissance vocale ou faciale, et tout autre type de biométrie.

Exemple : pour se connecter à sa section, il faut présenter un mot de passe et une empreinte digitale.

MFA (= authentification à facteurs multiples): Méthode qui exige, quant à elle, plus de deux preuves d'identité.

Au vu des informations sensibles (informations personnelles des clients) que possède l'entreprise, nous préconisons d'utiliser la méthode MFA pour avoir une très forte sécurité.

L'utilisateur aura donc à utiliser le lecteur d'empreinte digitale et le lecteur de carte Sim pour se connecter à sa session, puis il lui faudra un mot de passe pour se connecter aux services de travail à distance de l'entreprise.

En termes de sécurité pour le mot de passe, il devra au minimum comporter : 8 caractères, 1 majuscule, 1 minuscule, 1 chiffre et 1 caractère spécial. De plus le mot de passe devra être anonyme, c'est-à-dire qu'il ne doit pas contenir une information qui identifie la personne.

Ces mesures sont les mesures préconisées par le gouvernement.

Par conséquent, il faudra que l'ordinateur possède un lecteur d'empreinte et un lecteur de carte Sim. S'il n'y a pas de lecteur de carte Sim, il y a la possibilité d'en prendre un externe.

En plus de ces mesures de sécurité, nous préconisons d'utiliser un VPN pour se connecter aux services de télétravail et un anti-virus. Ainsi nous aurons une connexion sécurisée entre le collaborateur et l'entreprise.