Note Destinée aux Utilisateurs  	SAKO Bah/ AHMED Abdou / PAQUEMARD Aurélien 2B-SISR

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention	Mode de diffusion	Validateur
1.0	SAKO Bah/ AHMED Abdou / PAQUEMARD Aurélien	05/01/2024	3	Assurmer-IT	.pdf	SAKO Bah

Note Destinée aux Utilisateurs - Bonnes Pratiques pour un Déploiement Sécurisé :

Cher utilisateur,

Nous sommes ravis de vous informer que de nouveaux équipements seront déployés dans les prochains jours pour améliorer votre expérience de travail. Afin de garantir un déploiement en toute sécurité et une transition fluide, veuillez prendre en compte les directives suivantes :

1. Sécurité du Matériel :

- Assurez-vous que le nouvel équipement est utilisé conformément à sa destination professionnelle uniquement.

- Évitez de partager votre équipement avec des tiers non autorisés, même temporairement.

- Soyez prudent lors de l'utilisation en lieu public et veillez à toujours verrouiller votre session.

2. Identifiants et Authentification :

- Protégez soigneusement vos identifiants d'utilisateur, tels que le nom d'utilisateur et le mot de passe associé à votre compte. Ne les partagez jamais avec quiconque, même au sein de l'organisation. Respectez la note concernant les mots de passe.

- Évitez d'utiliser des informations personnelles ou facilement devinables comme mots de passe. Privilégiez des combinaisons complexes de lettres, chiffres et caractères spéciaux.

3. Sensibilisation à la Sécurité :

- Soyez vigilant face aux tentatives de phishing ou de fraude par courrier électronique. Vérifiez toujours l'authenticité des communications.

- Ne partagez jamais vos mots de passe ou informations personnelles via des canaux non sécurisés.

- Ne laissez pas vos identifiants enregistrés sur l'équipement ou dans des endroits accessibles à d'autres. Si vous suspectez une compromission, changez immédiatement votre mot de passe et signalez-le au service informatique.

4. Mises à Jour et Logiciels

- Ne tentez pas d'installer des logiciels par vous-même en raison des restrictions d'accès. Pour toute demande d'installation de logiciel supplémentaire nécessaire à votre travail, veuillez contacter le service informatique.

- Les mises à jour du système d'exploitation seront gérées par le service informatique. Veuillez suivre les directives fournies par le service informatique pour les redémarrages nécessaires à la suite de mises à jour.

5. Utilisation Responsable du Réseau :

- Respectez les politiques de sécurité réseau en vigueur dans notre organisation.
- Évitez de connecter des périphériques non autorisés à votre équipement.

6. Sauvegarde Régulière :

- Effectuez des sauvegardes régulières de vos données importantes. Suivez les procédures de sauvegarde recommandées par le département informatique.

7. Assistance Technique :

- Pour toute question technique, contactez le support informatique de l'entreprise. N'utilisez pas de services tiers sans autorisation préalable.

8. Communication avec le Département Informatique :

- Signalez tout comportement suspect ou toute activité anormale à l'équipe informatique.
- Informez immédiatement le service informatique en cas de perte ou de vol de votre équipement.

Merci de votre collaboration pour assurer la sécurité et la productivité de notre environnement informatique. En cas de doute ou de préoccupation, n'hésitez pas à contacter le service informatique.

Cordialement,

Assurmer, L'équipe Informatique