

 <p data-bbox="549 248 1002 286"><u>Bonnes pratiques et sécurité</u></p> <p data-bbox="563 524 922 647">Bonnes pratiques relatives à la sécurité de cet équipement</p>	<p data-bbox="1062 199 1390 376">HUYNH Michael BELAHA Sidhamed FRANCAIS Benjamin</p> <p data-bbox="1246 479 1390 517">1B-SISR</p>
--	---

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention	Mode de diffusion	Valideur
1.0	FRANCAIS Benjamin ; BELAHA Sidahmed; HUYNH Michael	10/01/2024	4	Assurmer-IT	.pdf	FRANCAIS Benjamin

INTRODUCTION :..... 3
Sécurité et bonnes pratiques..... 4
Charte Utilisateurs 4

INTRODUCTION :

Précédemment nous avons pour objectif de sélectionner des machines pour notre infrastructure informatique.

Le projet présent consiste à déployer efficacement les outils de travail sur l'ensemble des postes tout en garantissant la sécurité et la fiabilité des opérations.

Suite à la réception des équipements soigneusement choisis lors de l'analyse précédente, notre objectif actuel est désormais de mettre en place les outils nécessaires sur chaque poste utilisateur et d'organiser la remise de ces derniers.

Pour répondre à ces impératifs, nous aborderons plusieurs thèmes essentiels :

- Choix des outils de déploiement d'OS :

Nous présenterons deux outils de déploiement en mettant en avant leurs caractéristiques distinctives, leurs avantages et inconvénients respectifs, nous écarterons de notre champ de possibilité le déploiement à la clé USB.

- Sélection de l'outil retenu :

Nous justifierons notre choix d'outil de déploiement après avoir étudié ces derniers. Vous trouverez ci-joint une procédure de sa procédure d'installation sur des utilisateurs.

- Sécurité et bonnes pratiques :

Un volet crucial de notre mission consistera à informer les utilisateurs des bonnes pratiques à adopter pour garantir la sécurité des nouveaux équipements ainsi que les données.

- Gestion de la remise des équipements :

Nous allons élaborer des mesures afin de créer une communication efficace pour la distribution des équipements aux utilisateurs, respectant ainsi les délais impartis.

Sécurité et bonnes pratiques

Charte Utilisateurs

Chers utilisateurs,

Nous sommes ravis de vous présenter notre nouveau matériel et nous souhaitons vous rappeler quelques bonnes pratiques pour garantir sa sécurité ainsi que la vôtre. Veuillez prendre en compte les points suivants :

Mises à jour et correctifs : Assurez-vous que le matériel dispose des dernières mises à jour logicielles et des correctifs de sécurité. Effectuez régulièrement ces mises à jour pour maintenir un niveau de sécurité optimal. N'oubliez pas si vous avez un doute contacter la hot line du service informatique nous vous communiquerons les mises à jour pouvant créer des dysfonctionnements.

Gestion des mots de passe : Changez les mots de passe par défaut fournis avec le matériel et optez pour des mots de passe forts et uniques. Ne partagez jamais ces informations avec des tiers. Contactez la hot line si vous avez des problèmes de gestion de mots de passe.

Sauvegardes régulières : Effectuez des sauvegardes régulières des données stockées sur le matériel pour éviter toute perte en cas d'incident de sécurité.

Support technique et rapport d'incidents : En cas de demande ou problème, suspicion de violation de sécurité, contactez immédiatement le support technique et rapportez l'incident pour une action appropriée.

Chers utilisateurs afin d'assurer une traçabilité ainsi qu'un rapport complet sur chaque situation nous vous prions de rédiger des tickets via GLPI.

En suivant ces bonnes pratiques, vous contribuez à garantir la sécurité du nouveau matériel, préservant ainsi la confidentialité et l'intégrité des données. Votre coopération est essentielle pour maintenir un environnement sûr et fiable.

Merci de votre attention et de votre engagement envers la sécurité.

Cordialement,

L'équipe informatique d'Assurmer

N° de téléphone : xx xx xx xx xx

