A faire	En cours	Fait
		Préconisations sur un environnement de "masteurisation". *Alexandre*
		Procédure préparation d'un poste avant sa délivrance au visiteur. *Alexandre*
		Procédure à appliquer lors de la récupération d'un équipement pour reconditionnement ou pour réparation. Alexandre
		Une charte sur le bon usage de l'équipement. *Alexandre*
		Descriptif technique des caractéristiques matérielles de l'équipement. *Enzo*
		Trois propositions commerciales professionnelles avec une garantie d'un an. *Enzo*
		Une liste de solutions logicielles à installer et aussi afin de sécuriser physiquement et logiciellement les postes à disposition. *Enzo*
		Les éléments de configuration et de paramétrage à appliquer. *Enzo*

Préconisations pour un Environnement de Masteurisation

1. Introduction

La gestion des équipements destinés aux visiteurs nécessite un système de masteurisation efficace pour optimiser le suivi et la maintenance, garantissant ainsi une expérience enrichissante.

Objectif :
Ce document présente une analyse des choix technologiques, notamment la sélection entre des solutions avec ou sans serveur et les options logicielles (libres ou payantes).

---

2. Analyse des besoins

Utilisateurs

- **Visiteurs :** Accès aux informations sur les équipements**.**
- **Personnel technique :** Suivi des interventions et gestion de la maintenance.
- **Gestionnaires :** Analyse des données pour des décisions éclairées.

Fonctionnalités clés

- Suivi des interventions.
- Gestion des stocks.
- Rapports analytiques**.**

---

3. Choix technologique

Solutions avec serveur

Avantages :

- Centralisation des données.
- Sécurité accrue.
- Personnalisation possible.

Inconvénients :

- Coûts d'hébergement.
- Besoins techniques pour la gestion.

Solutions sans serveur (cloud)

Avantages :

- Coûts réduits d'infrastructure.
- Scalabilité.
- Mises à jour automatiques.

Inconvénients :

- Dépendance à Internet.
- Risques de sécurité des données.

---

4. Solutions logicielles

Solutions libres

Exemples :

- **GLPI :** Gestion des interventions et des actifs.
- **Snipe-IT :** Gestion des actifs matériels.

Avantages :

→ Coût nul.

→ Personnalisation.

Inconvénients :

→ Support limité.

→ Compétences techniques requises.

Solutions payantes

Exemples :

- **ServiceNow :** Gestion des services IT.
- **Freshservice :** Outil convivial pour la gestion des services.

Avantages :

→ Support technique dédié.

→ Fonctionnalités avancées.

Inconvénients :

→ Coûts d'acquisition.

→ Flexibilité limitée.

5. Recommandations

Critères de sélection

- **Coût total de possession :** Évaluer licences, maintenance et support.
- **Fonctionnalités :** Assurer que toutes les fonctionnalités nécessaires sont présentes.
- **Scalabilité :** Vérifier l'adaptabilité aux besoins futurs.
- **Support technique :** Analyser la qualité du support proposé.

Mise en œuvre

Phases recommandées :

1. **Installation :** Mise en place du serveur et du logiciel.
2. **Configuration :** Personnalisation de la solution.
3. **Tests : Validation** des fonctionnalités.
4. **Déploiement :** Formation des utilisateurs.

---

6. Conclusion

L'adoption d'un environnement de masteurisation est cruciale pour une gestion efficace des équipements et l'amélioration de l'expérience des visiteurs. En choisissant une solution adaptée, l'organisation pourra mieux gérer ses ressources et répondre aux attentes des utilisateurs.

Procédure de Préparation d'un Poste Avant Délivrance au Visiteur

Objectif

L'objectif de cette procédure est d'assurer que chaque poste est prêt, fonctionnel et conforme aux normes de sécurité et de qualité avant d'être remis à un visiteur. Une préparation rigoureuse garantit non seulement une expérience utilisateur optimale, mais minimise également les risques de problèmes techniques durant l'utilisation.

1. Vérification de l'Équipement

La première étape consiste à inspecter l'état physique du poste. Il est important de vérifier l'intégrité des composants tels que l'écran, le clavier, la souris et le boîtier. L'absence de dommages visibles, tels que des rayures ou des chocs, doit être confirmée. De plus, il convient de vérifier la configuration matérielle en s'assurant que tous les périphériques sont

correctement connectés et en testant la fonctionnalité de chaque composant, notamment l'écran, le son et les ports USB.

2. Mise à Jour et Configuration Logicielle

Une fois l'équipement vérifié, la prochaine étape est la mise à jour et la configuration logicielle. Cela inclut la vérification et l'installation des dernières mises à jour de sécurité pour le système d'exploitation. Il est également essentiel d'installer les applications nécessaires à l'utilisation prévue par le visiteur, en s'assurant qu'elles fonctionnent correctement et sont à jour. Enfin, les paramètres utilisateur doivent être configurés, ce qui peut inclure la création d'un compte temporaire et le paramétrage des préférences comme la langue et l'accès aux applications.

3. Vérification de la Sécurité

La sécurité de l'équipement est une priorité. Il est donc nécessaire de configurer les paramètres de sécurité, notamment en activant les protections antivirus et anti-malware, ainsi que le pare-feu. Il est également important de vérifier l'accès aux réseaux en testant la connexion au réseau Wi-Fi ou Ethernet et en s'assurant que les paramètres de sécurité du réseau sont en place pour protéger les données du visiteur.

4. Test Fonctionnel

Après avoir configuré le poste, il est essentiel d'effectuer un test fonctionnel complet du système. Cela implique de vérifier que tous les logiciels s'ouvrent et fonctionnent correctement, ainsi que de tester la connexion Internet et l'accès aux ressources en ligne. De plus, il convient de tester les fonctionnalités spécifiques requises par le visiteur pour s'assurer qu'elles fonctionnent comme prévu.

5. Documentation et Suivi

Une fois toutes les opérations effectuées, il est important de remplir une fiche de préparation. Ce document doit répertorier toutes les opérations réalisées, les configurations et les tests effectués, ainsi que toute observation ou anomalie rencontrée. Par la suite, il est crucial d'informer le personnel concerné des détails du poste préparé, en notant toute information pertinente sur son utilisation ou ses limitations.

6. Nettoyage et Finition

Pour conclure la préparation, le poste doit être soigneusement nettoyé. Cela inclut l'essuyage de l'écran, du clavier et de la souris pour garantir une présentation propre et agréable. Enfin, il est recommandé de préparer tout matériel d'accompagnement, comme des instructions d'utilisation ou un guide de dépannage, afin que le visiteur puisse utiliser le poste sans difficulté.

Procédure de Récupération d'un Équipement pour Reconditionnement ou Réparation

Objectif

L’objectif de cette procédure est d’assurer la récupération sécurisée et efficace des équipements destinés au reconditionnement ou à la réparation. En suivant ces étapes, on garantit non seulement la sécurité des données, mais aussi un traitement approprié des pannes et une remise en état de l’équipement, optimisant ainsi la durée de vie des ressources.

1. Sauvegarde des Données

La première étape essentielle avant toute intervention sur l'équipement est la sauvegarde des données. Cela consiste à identifier les données critiques, telles que fichiers, documents et configurations importantes, stockées sur le poste. Il est impératif d'effectuer une sauvegarde en utilisant des dispositifs de stockage externes ou des solutions de cloud, garantissant que toutes les informations nécessaires sont conservées. Une fois la sauvegarde effectuée, il est crucial de vérifier son intégrité en s'assurant que les données sauvegardées sont accessibles et utilisables, ce qui implique de réaliser des tests d’ouverture de fichiers.

2. Suivi des Pannes

Après avoir sécurisé les données, il est important de documenter toutes les pannes ou anomalies rencontrées avec l’équipement. Cela commence par enregistrer les symptômes observés, tels que des plantages, des lenteurs ou des erreurs d’affichage. Il est également conseillé d’effectuer des tests de diagnostic pour identifier les causes sous-jacentes des pannes. Tous les résultats de ces tests doivent être soigneusement documentés dans un rapport, qui servira de référence pour les actions à entreprendre lors de la réparation ou du reconditionnement.

3. Réinitialisation de l'Équipement

La réinitialisation de l’équipement est une étape clé pour le préparer au reconditionnement. Cette opération implique de remettre l’appareil à son état d’origine en suivant les procédures spécifiques de réinitialisation des paramètres d’usine. Parallèlement, il est nécessaire de désinstaller toutes les applications non essentielles et de s’assurer qu’aucune donnée personnelle ne reste sur le système. Une fois la réinitialisation effectuée, il convient de vérifier les mises à jour du système d’exploitation et d’installer les dernières versions des logiciels de base pour garantir un fonctionnement optimal.

4. Remise en État de l'Équipement

La dernière étape consiste à remettre l’équipement en état. Cela commence par une inspection physique minutieuse pour vérifier l’état des composants tels que l’écran, le clavier et le boîtier, en notant toute usure ou dommage. Ensuite, un nettoyage approfondi de l’appareil est effectué pour garantir une présentation soignée et fonctionnelle. Si des composants sont usés ou défectueux, ils doivent être remplacés pour s'assurer que l'équipement fonctionnera de manière optimale lors de sa prochaine utilisation.

5. Documentation Finale

Enfin, il est crucial de documenter l’ensemble du processus de récupération de l’équipement. Cela inclut la rédaction d’une fiche de suivi récapitulant toutes les actions entreprises, les pannes identifiées et les réparations effectuées. De plus, il est recommandé d’étiqueter l’équipement comme étant en cours de reconditionnement ou de réparation, en ajoutant la date et les détails pertinents de la procédure. Cette documentation permettra de suivre l’historique de l’équipement et d’assurer un suivi efficace lors des futures interventions.

Cette procédure de récupération d'équipement garantit un traitement systématique et sécurisé des postes destinés au reconditionnement ou à la réparation. En respectant ces étapes, l’organisation optimise la gestion de ses ressources tout en préservant la sécurité des données et en maximisant la durée de vie des équipements.

Charte de Bon Usage de l'Équipement

Cette charte a pour objectif de promouvoir une utilisation responsable et efficace de l'équipement mis à disposition des visiteurs. Elle vise à garantir la sécurité, le respect des biens et l’optimisation des ressources, tout en favorisant une expérience positive pour tous.

1. Responsabilité de l'Utilisateur

Chaque utilisateur est responsable de l’équipement qui lui est confié. Il est impératif de traiter chaque poste avec soin et de signaler immédiatement toute anomalie ou dommage constaté. Les utilisateurs doivent être conscients que leur comportement influence directement la qualité de l'équipement et l'expérience des autres visiteurs.

2. Utilisation Conforme

L’équipement doit être utilisé exclusivement à des fins prévues. Toute utilisation inappropriée, telle que le téléchargement de logiciels non autorisés, la modification de paramètres système ou l’accès à des sites inappropriés, est strictement interdite. Les utilisateurs doivent également respecter les politiques de sécurité et de confidentialité en vigueur.

3. Hygiène et Propreté

Les utilisateurs doivent veiller à maintenir l’équipement et l’espace de travail propre et rangé. Il est recommandé de ne pas manger ou boire à proximité des postes afin de prévenir tout dommage. Après utilisation, chaque utilisateur est prié de nettoyer l'équipement (écran, clavier, etc.) et de s’assurer que l’espace est prêt pour le visiteur suivant.

4. Sauvegarde et Protection des Données

Il est de la responsabilité de chaque utilisateur de sauvegarder ses données personnelles et de ne pas stocker d’informations sensibles sur les équipements. Les utilisateurs doivent également respecter les réglementations en matière de protection des données et de confidentialité.

5. Formation et Assistance

Les utilisateurs sont encouragés à suivre les formations disponibles sur l’utilisation des équipements et à demander de l’aide au personnel en cas de besoin. En cas de difficultés techniques, il est préférable de solliciter l’assistance plutôt que d’essayer de résoudre les problèmes par soi-même, ce qui pourrait endommager l’équipement.

6. Respect des Autres Utilisateurs

Chaque utilisateur doit faire preuve de courtoisie envers les autres visiteurs. Il est important de maintenir un environnement calme et propice à la concentration. Les utilisateurs sont priés de respecter le temps d'utilisation accordé et de ne pas monopoliser l'équipement au détriment des autres.

Cette charte de bon usage de l'équipement a pour but d'assurer une utilisation respectueuse et efficace des ressources mises à disposition. En respectant ces principes, chaque utilisateur contribue à une expérience positive pour tous et à la durabilité des équipements. Toute violation de cette charte pourra entraîner des sanctions appropriées, pouvant aller jusqu'à l'interdiction d'accès aux équipements.

Solutions Logicielles pour les Visiteurs

1. **Suite Bureautique**
    - LibreOffice ou Microsoft Office 365 : Pour le traitement de texte, les tableurs et les présentations.
2. **Navigateurs Internet**
    - Google Chrome ou Mozilla Firefox : Pour une navigation rapide et sécurisée.
3. **Applications de Prise de Notes**
    - Evernote ou Microsoft OneNote : Pour la prise de notes et l'organisation des idées.
4. **Lecteurs Multimédias**
    - VLC Media Player : Pour la lecture de fichiers audio et vidéo.

Outils de Sécurisation Physique et Logicielle

1. **Logiciels de Sécurité**
    - Antivirus (ex. : Bitdefender, Norton) : Pour protéger contre les malwares et virus.
    - Pare-feu (ex. : ZoneAlarm, intégré au système d'exploitation) : Pour contrôler le trafic réseau.
2. **Solutions de Sauvegarde**
    - Acronis True Image ou Backblaze : Pour des sauvegardes régulières des données critiques.
3. **Gestion des Accès**
    - LastPass ou 1Password : Pour la gestion sécurisée des mots de passe.
4. **Chiffrement des Données**
    - VeraCrypt ou BitLocker : Pour chiffrer des données sensibles sur le disque dur.
5. **Systèmes de Contrôle d'Accès Physique**
    - Verrous électroniques ou badges d'accès : Pour restreindre l'accès aux équipements.
6. **Outils de Surveillance**
    - Caméras de sécurité ou logiciels de monitoring : Pour surveiller physiquement l'accès aux postes.
7. **Solutions de Gestion de l'Infrastructure IT**
    - ServiceNow ou GLPI : Pour la gestion des incidents et la maintenance des équipements.

Conclusion

Cette liste de solutions logicielles et d'outils vise à offrir aux visiteurs une expérience productive tout en garantissant la sécurité des postes à disposition. L'implémentation de ces outils aidera à maintenir un environnement de travail sûr et efficace.

Enzo

1)

D’après mon point de vue il serait préférable de prendre des ordinateurs fixe dû au fait que les ordinateurs ne sont pas destinés à un usage personnel donc cela permettra de laisser les ordinateurs à la même place.
Le fait d’avoir des ordinateurs fixes sera un confort supplémentaire pour les employés avec par exemple des écrans plus grands, un clavier plus ergonomique pour le traitement de texte etc …
il sera capable de faire tourner tous les logiciels de bureautique sans problème, ainsi que de la navigation web.

Listes composants pour l’ordinateur standard pour la M2L:

- **Ordinateur Fixe**

- Intel i3 ou i5 / AMD ryzen 5
- minimum 8go ram
- minimum ssd 480go
- prises USB 2.0/3.0 HDMI, RJ45
- carte réseau
- Microsoft Windows 11 Pro

2)

Pour la liste du matériel voir tableur liste matériel.

1. **Lien des produits**

- **Proposition 1:**

https://www.ldlc.pro/fiche/PB00593326.html

https://www.ldlc.pro/fiche/PB00609374.html

- **Proposition 2:**

https://www.ldlc.pro/fiche/PB00592339.html

https://www.ldlc.pro/fiche/PB00609374.html

- **Proposition 3:**

https://www.ldlc.pro/fiche/PB00588343.html

https://www.ldlc.pro/fiche/PB00609374.html

4)

1. **Les logiciels de sécurité:**

- **Anti-virus**

Tout d'abord, nous aurons besoin de logiciels de sécurité tels que Windows Defender qui est présent de base sur les ordinateurs proposés.

Mais nous pouvons aussi rajouter un autre anti-virus comme Bitdefender ainsi que Malwarebytes permettant de scanner et retirer les logiciels malveillants.

- **Logiciels de chiffrement des données**

  - VeraCrypt
  - BitLocker

  Ces deux logiciels ont la même utilité qui est le chiffrement des données.

2. Sécurité physique:

Pour ce qui est de la sécurité physique les postes nous pouvons utiliser
Des serrures RFID ce qui permettrait de contrôler l'accès aux postes.
Ou même ajouter des caméras de surveillance.

3. Logiciels de bureautique

- **Navigateur :**
  - Chrome, FireFox etc …

- **Traitement de texte, tableurs …**

  - LibreOffice
    → avantages : Gratuit
    → inconvénients : moins d'options qu'un logiciel payant
  - Pack Microsoft Office
    → avantages : Plus d'options
    → inconvénients : Prix
  - Adobe Acrobat

3)

1. Définition d'une nomenclature pour nommer les équipements

Il est essentiel de suivre une nomenclature cohérente pour faciliter la gestion et l'identification des équipements. La RFC 1178 propose plusieurs recommandations, telles que :

- **Utilisation de noms descriptifs** : Inclure des informations sur la fonction de l'équipement (ex. : `srv-web-01` pour un serveur web).
- **Conformité aux conventions de nommage** : Éviter les caractères spéciaux et respecter la longueur maximale des noms.
- **Consistance** : Appliquer la même logique de nommage à tous les équipements.

- **exemple de création du nom d’un équipement :**

  B[code bâtiment]E[numéro étage]L[numéro ligue]S[numéro salle].P[numéro poste]

  Code bâtiment qui peut être A ou C
  - N° étage est compris entre 1 et 4 (puisque les locaux du rez-de-chaussée n'hébergent pas de ligues)
  - N° ligue sur 2 chiffres : correspond à un nombre attribué à la ligue allant pour l'instant de 01 à 24
  - N° salle sur 2 chiffres : correspond aux bureaux occupés par les ligues
  - N° poste sur 2 chiffres : correspond au numéro écrit sur la prise murale

  Exemple : le nom d'hôte BAE2L06S01P01 correspond au poste installé sur la prise N°1 du bureau A201 occupé par la ligue de Volley, bureau situé au deuxième étage du bâtiment A

2. Comptes à créer

Les comptes d'utilisateur doivent être bien définis pour garantir la sécurité et la gestion des accès :

- **Comptes administratifs** : Pour les administrateurs système, avec des droits d'accès étendus.
- **Comptes utilisateurs** : Pour les utilisateurs finaux, avec des permissions limitées selon leurs besoins.
- **Suivi des activités** : Mettre en place un système de journalisation pour suivre les connexions et les actions des utilisateurs.

3. Sécurisation des accès et des données

La sécurisation est cruciale pour protéger les ressources :

- **Authentification forte** : Utiliser des méthodes d'authentification à deux facteurs (2FA).
- **Politiques de mot de passe** : Exiger des mots de passe complexes et un changement régulier.
- **Chiffrement des données** : Appliquer le chiffrement pour les données sensibles en transit et au repos.

4. Paramétrages réseaux éventuels

Il est important de configurer correctement les paramètres réseaux :

- **Segmentation du réseau** : Créer des sous-réseaux pour séparer les différentes fonctions (ex. : administration, utilisateurs).
- **Pare-feu et règles de filtrage** : Mettre en place des règles pour contrôler le trafic entrant et sortant.

- **Surveillance du réseau** : Utiliser des outils de surveillance pour détecter les anomalies.

5. Organisation de l'espace de stockage

L’organisation de l’espace de stockage doit être réfléchie :

- **Stratégie de sauvegarde** : Établir une routine de sauvegarde régulière et tester les restaurations.
- **Hiérarchisation des données** : Classer les données par priorité et par type pour optimiser l’accès et le stockage.
- **Contrôle des accès** : Définir des permissions d'accès pour les différents types de données.

Conclusion

En suivant ces recommandations, on peut assurer une configuration et un paramétrage efficaces et sécurisés des équipements. Il est important de réévaluer régulièrement ces éléments pour s’adapter aux évolutions technologiques et aux besoins de l'organisation.