Conseils Must >> Recommandations

SAUVEGARDE DES DONNÉES

www.mustinformatique.com

Matériels : sécurité & sauvegardes

Les conseils de notre équipe Système & Réseaux

- **S'assurer que les différentes données de production font l'objet d'une sauvegarde**
  - Base de données de Must G5
  - Comptabilité
  - Messagerie
  - Serveur de fichiers

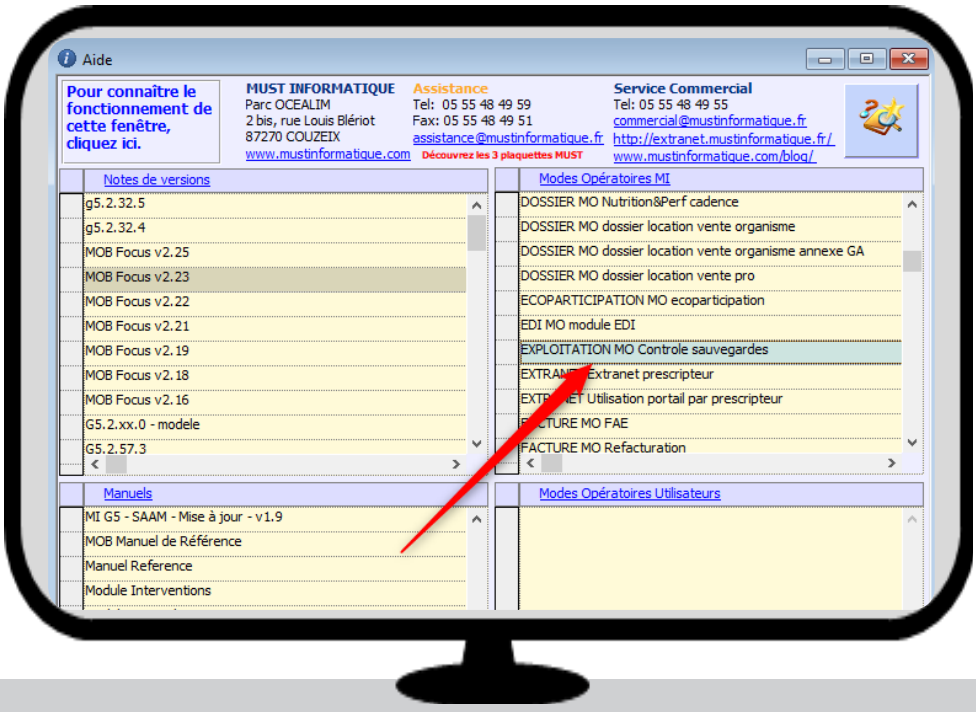
- **S'assurer que le ou les programme(s) sont correctement automatisés pour effectuer une sauvegarde journalière à minima.**

- **Supports de sauvegarde préconisés**
  - Il est nécessaire de sauvegarder sur des supports différents à chaque sauvegarde
  - Ne pas stocker vos sauvegardes au même endroit que le/les serveurs
  - Il est nécessaire d'externaliser les supports de sauvegarde le plus régulièrement possible (une par semaine au moins / chaque jour au mieux)
  - Il est nécessaire que l'ensemble des PC et serveurs soit protégé par un anti-virus à jour
  - Il est possible d'effectuer des sauvegardes sur différents supports : disque USB, externalisé,...
  - Il est nécessaire de sauvegarder les documents à conserver.

- **Vérifier le contenu de la sauvegarde**
  - Le fichier **« orthop.backup »** (c'est le nom standard, mais votre sauvegarde peut comporter un autre nom) est le Dump de votre Base de Données principale.
  - Celui-ci doit obligatoirement être présent et de taille conséquente (> 10Mo et peut en faire plusieurs centaines).
  - De plus, la **taille des dump** va en progressant (sauf suppression de données dans la BDD), elle doit donc être plus importante (ou égale s'il n'y a pas eu de création dans la BDD) dans le 1 que dans le 2 et dans le 2 que dans le 3…
  - En plus de la taille, on **contrôle la date de modification.** Celle-ci doit correspondre à la date de la dernière exécution du script.

- **Document détaillé téléchargeable depuis Must-G5 | Aide | Aide : partie Modes Opératoires MI**

- **Nom du document "EXPLOITATION MO Contrôle sauvegardes"**



Quelques règles de prudence

→ Présence de programmes malveillants = se prémunir des cyber-attaques

- Disposer d'un pare-feu et anti-virus performants
- Prendre en compte les alertes
- Vérifiez ses accès personnels

→ Botnets = programmes malveillants pouvant paralyser les serveurs (exemples : rendre inutilisable une plateforme e-commerce ou bloquer une boite de réception)

- Activer la mise à jour automatique à l'intégralité du parc informatique
- Utiliser un anti-virus et un firewall
- Sensibiliser les employés aux risques
- Veiller à la mise à jour des logiciels

→ Reflexe à adopter lors de la réception de courriels

- **Vérifier le nom de l'expéditeur** avec pièce jointe, liens, forme du mail inhabituelle. Partez du principe que tout interlocuteur potentiel, même s'il n'est pas malveillant, peut infecter votre boite mail par un simple envoi de mails comportant des virus.
- **Se méfier des pièces jointes**, faites attention aux demandes d'informations confidentielles, restez vigilant aux liens
- **Paramétrer ses logiciels de messagerie** : activer la procédure de mise à jour automatique, désactiver la prévisualisation automatique des courriels, bloquez l'exécution automatique des ActiveX, des plugins et des téléchargements, utiliser un éditeur de texte pour ouvrir vos pièces jointes.

MUST INFORMATIQUE
Parc d'activité Océalim
20 avenue Maryse Bastié
87270 Couzeix

CONTACT

05 55 48 49 55
commercial@mustinformatique.fr
www.mustinformatique.com