

Ordinateurs « blancs » à la MMSH

Mise en place d'un service d'ordinateurs dédiés aux missions à la MMSH

Simon Moré - VVT 2026

26 juin 2026

UAR Maison **Méditerranéenne** des Sciences Humaines et Sociales

10 UMR SHS associées (archeo, histoire, socio, politique, anthropo), 2 instituts,
1 point commun : la Méditerranée (spécialisé mondes arabes)

—> Contexte géopolitique compliqué. . .

Et des missionnaires militants, chercheurs en contrats PAUSE (Programme Accueil en Urgence des Scientifiques Exilés) ou Safe Place For Science.

Enjeux des missions “à risque”

- Enjeux de sécurité des personnes
- Enjeux de sécurité SI : un poste est un point d'entrée sur le S.I.
- Enjeux diplomatiques.



Je n'ai rien à cacher

- Discussions avec le D.U de la possibilité et pertinence d'un ordi blanc sans données.
- Discussions au sein du service info : qu'est ce qu'on configure ou pas. Comment ?
- Discussions avec les gestionnaires sur l'organisation : On ne peut pas gérer les ordis blancs de 10 unités (stockage, reservations, etc. . .).
- Discussions avec les premiers missionnaires équipés

Patrick Barkate, FSD AMU :

*Il est rappelé qu'il est important de ne pas partir avec son matériel habituel, mais **d'utiliser un poste banalisé** ne contenant que les données nécessaires à la mission et aucune donnée sensible.*

Jérôme Vitre, Délégué régional du CNRS

Dans le contexte international actuel, et suite à l'incident rencontré par un chercheur CNRS à l'entrée aux USA, le HFDS (haut fonctionnaire Défense et Sécurité) du MESR a transmis les rappels suivants :

*[...] La meilleure des solutions (et la préconisation constante du FSD et du RSSI en termes de PPST et de SSI) est de **partir avec portable et PC dédiés aux missions**, vides de toute messagerie et de tout document sensible...*

Concrètement un poste sans données ?

- Un point d'accès sécurisé aux services cloud institutionnels (webmail, amubox, sDrive, visio dans le navigateur : via VPN)
- Sans lien avec la MMSH. Pas dans le domaine ni le parc, ni sur notre réseau ni sur notre VPN, ni sur notre anti-virus.
- Chiffré pour les vols mais avec clé dans les bagages à fournir sur demande des autorités.
- Avec les outils de base : bureautique , audiovisuel
- Utilisateur administrateur du poste, compte « voyageur »
- Ordi entrée de gamme MATINFO sans etiquette

- Déploiement (WAPT) de notre image Windows avec config ordi blanc
 - Procédure **simple** :
- 0 L'unité achète et gère le stockage et les réservations du poste
 - 1 Déploiement juste avant la Mission,
 - 2 remise au voyageur avec topo sensibilisation SSI (1h)
 - 3 au retour : formatage SSD depuis le Bios (avertir au moins 3 fois sur la perte de données). Et restitution au labo.
- > poste inutilisable pour des stagiaires

- Sensibilisation des risques SI (on ne fait pas de politique)
- Sensibilisation données sensibles (PPST, contacts, identifiants)
- Sensibilisation aux dangers des outils non institutionnels
- Sensibilisation Mot de Passe connaître ses mots de passe (pas de gestionnaire sur ordi blanc) —> la difficulté n°1... Choisir un mot de passe simple à retenir mais robuste Modification au retour
- Sensibilisation smartphone
- Sensibilisation aux bonnes pratiques (phishing, comportement, pro/perso, choix du wifi)

Objectif : protéger le plus possible les personnes et le S.I.

Résultat : Ça marche bien, tous contents de la procédure, missionnaires rassurés, D.U responsables, S.I. protégé, consignes respectées.

Un moment privilégié pour la sensibilisation

Aujourd'hui 4 labos équipés + 2 en cours dont 1 à moitié

- Pour les mac ? Pas de retour sur le mac blanc parti en mission. Formatage ?
- Pour les ZRR ?

- Des mots de passe robustes j'utiliserai
- Mes mots de passe par cœur je connaîtrai
- Mes mots de passe jamais je ne sauvegarderai
- Mes mots de passe jamais je ne partagerai
- Mon ordinateur, des yeux jamais je ne lâcherai
- Le VPN AMU j'utiliserai
- Des sauvegardes régulières je ferai
- De tous les mails je me méfierai
- Sur aucun lien douteux je ne cliquerai
- Aucun fichier douteux je n'ouvrirai