RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Inserm
La science pour la santé
From science to health

Recommandations lors de missions de courtes durées à l'étranger

Les conseils qui suivent ne doivent pas être perçus comme une contrainte administrative supplémentaire mais comme l'assurance que les risques auxquels vous êtes exposés en mission sont pris en compte et assumés.

Avant la mission

Un mois avant la mission

- Consulter le site du ministère des affaires étrangères (MEAE), conseils aux voyageurs et notez les **conditions particulières** (visa, vaccins), les **risques** (sociétaux, sanitaires…).
  http://www.diplomatie.gouv.fr/fr/conseils-aux-voyageurs/
- Vérifier la validité du **passeport** et notamment la date d'expiration supérieure à 6 mois par rapport à la date de retour.
- Vérifier la nécessité d'un **visa** en fonction du pays visité (ex. ESTA pour les US).
- Etablir un **ordre de mission.** Indispensable, pour la prise en charge financière et l'assurance de la mission.
- Saisir l'avis du Fonctionnaire Sécurité Défense (FSD) pour les pays à risques (**pays « jaune », « orange » et « rouge »** dans la classification du MEAE).
- Prévoir une **visite médicale** pour évaluer votre état de santé, recevoir les conseils d'hygiène, mettre à jour votre carnet vaccinal et établir les ordonnances de médicaments.

Quelques jours avant le départ

- Se déclarer sur le portail du ministère des Affaires étrangères « **Ariane** », relever le numéro de l'ambassade de France ;
  https://pastel.diplomatie.gouv.fr/fildariane/dyn/public/login.html
- Disposer d'une **assurance** complémentaire et d'un numéro d'appel d'urgence (assurance personnelle ou assurance prise avec la mission par l'INSERM).
- Faire une **copie papier** de ses pièces d'identité et numéros utiles.
- Prévoir le **budget** pour les frais de déplacement (transport, hébergement).
- Acheter pour le séjour les **médicaments** du traitement prophylactique ou préventif.
- Contacter et **prévenir vos partenaires étrangers** de votre arrivée. Demander toujours au partenaire sur place de vous attendre à l'aéroport si cela lui est possible ou prévoir avec lui une procédure claire à votre arrivée.

Lors du départ

- Emporter les **documents indispensables seulement** : passeport, carnet de vaccination, ordre de mission, lettre d'invitation, attestation de matériels transportés, liste des numéros utiles…
- Emporter uniquement les **documents professionnels en relation avec votre mission.**

- Si possible, **n'utilisez pas vos équipements électroniques habituels**, mais des équipements dédiés uniquement pour les missions[1]. Notamment, n'emportez pas votre boîte aux lettres, ni votre carnet d'adresse électronique, ni des résultats de recherche non protégés : votre disque dur peut être copié, directement ou lors d'une connexion de votre ordinateur au réseau de l'hôtel par ex.
- Sécuriser vos données scientifiques[2]**.**
- Installer un filtre de confidentialité sur l'écran de votre ordinateur.
- Éviter d'emporter des clés USB ou des disques durs externes.
- Mettre un signe distinctif sur vos appareils (ex. pastille de couleur) afin de mieux surveiller le matériel et de s'assurer qu'il n'y a pas eu d'échange, notamment pendant le transport.

Pendant la mission

Respecter les règles élémentaires de prudence et de sécurité

- **Eviter de voyager seul**.
- Observez strictement les formalités d'entrée et de séjour, en évitant notamment toute atteinte à la réglementation sur l'importation et l'exportation des devises. L'importation d'objets, livres, revues, voire de denrées doit se limiter aux seuls besoins personnels dans les pays où leur détention est réglementée.
- Lors des démarches administratives, vérifiez que l'on vous rend bien toutes les pièces que vous confiez.
- Ne laissez jamais des documents de travail importants dans des bagages sans surveillance ;
- Gardez avec vous les documents et supports magnétiques ou électroniques sensibles ou conservez-les dans une mallette fermée à clé. Il vous est de plus recommandé de chiffrer les documents ou supports transportant des informations sensibles. **Les principaux risques liés au nomadisme sont le vol ou la perte de l'équipement**.
- Ne transportez pas de lettres ou de paquets à titre de « service amical » car cela peut motiver une inculpation pour espionnage ou activité subversive. De même, n'acceptez pas de cadeau d'inconnus ou de personnes dont vous n'êtes pas totalement sures. Ces demandes de service ou ces cadeaux peuvent être effectués dans une intention de compromission.
- Evitez de prendre des notes en dehors de l'objet de la mission au cours de visites d'établissements scientifiques ou industriels ; cette pratique attire très fréquemment l'attention des services de sécurité.
- Evitez d'avoir des conversations importantes ou confidentielles dans une chambre d'hôtel ou chez un particulier. Les locaux d'hébergement ne garantissent pas contre les indiscrétions.
- En téléphonant ou en écrivant un message électronique, exprimez-vous en considérant que la transmission a de fortes chances d'être interceptée.
- Soyez prudent dans vos relations d'apparence amicales qui pourraient se nouer à l'occasion de ces voyages ; les services spécialisés ne répugnent pas à utiliser de tels moyens d'approche. De même, les guides et interprètes sont généralement en contact avec les services de renseignement auxquels ils sont souvent contraints de prêter leur concours.
- Accueillez avec circonspection les confidences de personnes se disant opposées au régime ou à la politique du gouvernement ; elles peuvent n'être que provocation.

[1] Contacter votre correspondant sécurité des systèmes d'information (CSSI).
[2] Liste des mesures en annexe.

Limiter les prises de risque sanitaire selon le pays

- Lavage des mains (gel), eau embouteillée, légumes cuits…
- Protection contre le soleil (crème, lunettes, vêtements), contre les IST (préservatifs), déshydratation (eau en bouteilles capsulées), les insectes (répulsifs, moustiquaire)
- Prise régulière d'antipaludéen et/ou autres traitements préventifs.

Après la mission

- Rapportez à votre hiérarchie ou à votre fonctionnaire de sécurité de défense (FSD) tout élément notable relatif à la sécurité, qu'il vous ait concerné ou qu'il puisse concerner des collègues.
- **Changez les mots de passe que vous avez utilisés pendant votre voyage. Analysez ou faites analyser vos équipements**.
- Rédigez un bref compte-rendu sous forme de document (électronique/papier) qui sera transmis au référent/encadrant et au directeur de l'Unité.
- Ne pas oublier de poursuivre jusqu'au terme prescrit la chimioprophylaxie préventive.
- Toute fièvre ou diarrhée au retour d'un séjour en zones tropicales nécessite une consultation chez un médecin.

ANNEXE : LISTE DES MESURES DE SECURISATION DES DONNEES NUMERIQUES

1. Imposer un mot de passe robuste (>12 caractères) au démarrage de la machine (mot de passe de « boot »).
2. Dissocier le compte administrateur du compte utilisateur dont les droits seront restreints afin de limiter les risques d'installation de logiciels non autorisés.
3. Surveiller de manière constante son ordinateur portable. Eviter de le laisser dans le coffre de sa voiture, dans une chambre d'hôtel, ou dans une salle de travail même pendant les pauses.
4. Restreindre l'usage des périphériques (lecteurs de disques, ports USB...). Désactiver la fonction *autorun* afin d'éviter l'exécution automatique d'un programme sans vérification préalable.
5. Toujours avoir un antivirus à jour (aussi bien pour les virus, que pour les logiciels espions) et scanner systématiquement tout support numérique extérieur ; **refuser la connexion d'équipements dont on ne connaît pas leur provenance (ex. USB offertes ou autres goodies).** Ils peuvent contenir des logiciels malveillants en développement non détectés par les antivirus ;
6. Mettre en œuvre une solution de communication sécurisée avec la métropole (VPN professionnel - réseau privé virtuel).
7. Instaurer un verrouillage automatique de la session après un certain délai d'inactivité (*i.e.* déverrouillage par mot de passe robuste). Eteindre l'ordinateur lorsqu'inutilisé ;
8. Désactiver le Bluetooth et le Wi-Fi de ses appareils nomades pendant les déplacements pour empêcher toute tentative de communication indésirable (ne les activer que lorsque nécessaire).
9. Utiliser votre chargeur personnel pour recharger ses équipements (la sécurité des bornes en libre-service n'est pas garantie).
10. Mettre en œuvre une solution de **chiffrement certifiée des données sensibles**[3] (rappel : OBLIGATOIRE pour les données cliniques, surtout si envoi par courriel).
11. Accéder à la messagerie Inserm uniquement via webmail.
12. Ne pas consulter les sites internet réputés dangereux avec son ordinateur professionnel (jeux en lignes, sexe, streaming...).
13. Attention à l'utilisation des photocopieurs numériques car ils disposent d'un disque dur gardant en mémoire les documents traités.

[3] Données personnelles, de santé, relatives aux systèmes d'information, aux marchés publics, ou aux recherches menées au sein de laboratoires protégés au titre de la protection du potentiel scientifique et technique de la Nation (PPST) (liste non exhaustive).

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

Inserm

La science pour la santé
From science to health