GUIDE

Sécurité numérique des déplacements professionnel à l'étranger

Quel risques ? Les voyages à l'étranger exposent les équipements et données professionnelles à des risques accrus de vol, d'espionnage ou de compromission. Certains pays peuvent intercepter ou altérer les connexions et les appareils. Une préparation rigoureuse et le respect des règles de sécurité sont donc essentiels pour préserver la confidentialité des informations.

Introduction

Les présentes recommandations viennent compléter les dispositions de la Charte de bonne conduite en matière d'utilisation des ressources informatiques de l'État.

Elles précisent les mesures à appliquer avant, pendant et après un déplacement à l'étranger, en particulier lorsque des équipements ou des données professionnelles sont emportés.

Les règles décrites ci-après s'appuient notamment sur les sections suivantes de la Charte de bonne conduite :

- Section 1.3 – Déplacement national : bonnes pratiques générales relatives à la protection des équipements et des données.
- Section 1.4 – Déplacement à l'étranger : consignes de sécurité spécifiques applicables en dehors du territoire national.
- Section 3.1 – Postes de travail et ordinateurs portables : exigences relatives à la protection, la configuration et l'utilisation des équipements informatiques de l'État.
- Section 2.3 – Accès distant et télétravail : conditions d'utilisation du VPN et des connexions à distance sécurisées.

Ces recommandations ne se substituent pas à la Charte de bonne conduite, mais en constituent une extension opérationnelle, adaptée aux contextes de déplacement et de missions à l'étranger. En cas de contradiction, les dispositions de la Charte prévalent.

Contactez-nous

En cas de question ou de besoin d'accompagnement concernant l'application du présent document, le HCPN/ANSSI, se tient à votre disposition. Pour toute demande, vous pouvez nous contacter, par courriel : support@anssi.etat.lu ou par téléphone : 247-88900.

Où trouver nos informations ?

L'ensemble de nos informations, documents et outils est accessible en ligne sur notre Extranet ANSSI ou notre GovSpace.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information

1. Avant le départ

- Prendre connaissance de la législation nationale applicable au pays visité.
- S'assurer que les données professionnelles non publiques seront consultées via des connexions sécurisées, et ne seront stockées localement que si cela est indispensable (par exemple en cas d'absence de connexion fiable sur place).
- Veiller à ce que les données professionnelles emportées soient chiffrées (ordinateur avec disque chiffré, clé USB chiffrée, etc.).
- Désactiver par défaut toutes les connexions sans fil (Wi-Fi, Bluetooth, NFC, partage de connexion, etc.) avant l'arrivée dans le pays, et les maintenir désactivées lorsqu'elles ne sont pas strictement nécessaires, afin de réduire l'exposition du matériel.
- Préparer des enveloppes scellées pour transporter le matériel informatique professionnel ou privé afin de s'assurer qu'il n'a pas été inspecté, modifié, échangé par un tiers.

Pour un voyage dans un pays à risques élevés

- Laisser le smartphone professionnel au Luxembourg afin d'éviter toute compromission. Si l'utilisateur souhaite apporter son téléphone personnel (p.ex. pour des photos) il est recommandé de le laisser en mode « offline » ou « avion » pendant la durée du séjour.
- L'utilisateur devrait travailler uniquement hors ligne, sans aucune connexion Internet. Un matériel "jetable" (Burner Phone / Burner PC) devrait être utilisé :
    * Le CTIE propose des Burner Phone pour le remplacement temporaire d'un smartphone professionnel pour la durée du voyage. La demande des Burner Phone peut se faire à travers une Service Request dans AskSAM.
    * Si nécessaire, prévoir également un ordinateur portable dédié (Burner PC) ne contenant aucune donnée sensible et utilisé uniquement pour la prise de notes locale. Le Burner PC sera formaté au retour de l'utilisateur.
- Préparer des mots de passe temporaires, qui seront obligatoirement changés au retour.
- N'emporter aucune information qui ne soit pas strictement nécessaire à la mission (documents, clés USB, mails archivés, etc.).

2. Pendant le voyage

- L'utilisateur demeure responsable de la protection physique de ses équipements et données tout au long du déplacement. Les dispositifs ne devraient jamais être laissés visibles ou sans surveillance, notamment dans des véhicules ou lieux publics, afin d'éviter tout vol, toute détérioration ou tout accès non autorisé.
- Les données professionnelles non publiques devraient être consultées via des connexions sécurisées (VPN). Si cela n'est pas possible, seules les données strictement nécessaires au besoin métier devraient être stockées localement et de manière sécurisé (chiffrement).
- Ne jamais connecter un ordinateur portable ou un smartphone à une prise USB publique ou inconnue, ni à des périphériques, supports ou réseaux externes non sécurisés. L'usage des chargeurs USB publics (aéroports, hôtels, bornes de recharge, etc.) est fortement déconseillé: seul un chargeur secteur personnel ou professionnel devrait être utilisé. Des enveloppes scellées peuvent être fournies si nécessaire pour le transport du matériel.
- Utiliser un filtre de confidentialité et ne pas utiliser l'ordinateur dans un environnement où l'écran pourrait être observé par des tiers (avion, train, hall d'hôtel, restaurant, etc.).
- Éteindre l'ordinateur portable pendant les déplacements.
- Lorsqu'un réseau Wi-Fi ou filaire inconnu ou non sécurisé est utilisé, la connexion directe à Internet est interdite. Seule l'utilisation du VPN professionnel est autorisée ; si la connexion VPN échoue, le réseau ne devrait pas être utilisé.
- En cas de perte ou de vol de matériel, prévenir au plus vite l'instance gestionnaire des incidents de sécurité et établir une déclaration dans un commissariat de police du pays dans lequel l'incident s'est produit.
- En cas de suspicion de compromission ou en cas d'inspection par les autorités locales, prévenir au plus vite l'instance gestionnaire des événements et des incidents de sécurité et agir selon les instructions communiquées.

Pour un voyage dans un pays à risques élevés

- L'utilisateur devrait utiliser exclusivement les équipements fournis pour la mission (Burner Phone et/ou Burner PC).
- L'utilisateur devrait travailler exclusivement en local. Il ne devrait donc ni se connecter à un réseau Wi-Fi, ni à Internet, ni aux services de l'État (ex. webmail, VPN, etc.).
- Limiter l'usage des appareils personnels, y compris pour un usage privé, afin d'éviter tout risque d'accès non autorisé, de copie de données ou d'infection.
- Il est recommandé d'éteindre le téléphone portable personnel pendant les déplacements.
- Ne pas utiliser WhatsApp, WeChat, Telegram ou toutes autres messageries non validées pour des échanges professionnels.

3. Au retour

- En cas de doute sur l'intégrité du matériel (ex. branchement sur un réseau non fiable, inspection par une autorité étrangère, comportement suspect de l'appareil), demander une analyse du poste au service informatique.

Pour un voyage dans un pays à risques élevés

- Restituer le Burner Phone et/ou le Burner PC au CTIE pour contrôle et réinitialisation complète.
- À votre retour, aucune donnée provenant du Burner Phone et/ou Burner PC ne devrait être transférée dans les systèmes de l'État sans analyse préalable et être dûment autorisée.
- Changer vos mots de passe temporaires préalablement définies : ils peuvent avoir été interceptés à votre insu.

LE GOUVERNEMENT
DU GRAND-DUCHÉ DE LUXEMBOURG
Haut-Commissariat
à la protection nationale

Agence nationale de la sécurité
des systèmes d'information