CRISEHELP
RISQUES - GESTION ET COMMUNICATION DE CRISE

Check-list Voyages à l'Étranger

Sécurité économique & numérique – Version universelle (tous pays)

Instructions pour utilisation

1. **Adaptation** : Personnalisez les sections selon vos besoins (pays, types de voyage ...).
2. **Format** : Imprimez ou intégrez dans un outil numérique (Excel, Teams) pour un accès facile. NE VOYAGEZ PAS AVEC CETTE VERSION
3. **Test** : Validez cette checklist lors de simulations pour en confirmer l'efficacité.

1. Mini-checklist conceptuelle

- Définir les **actifs sensibles** et minimiser les données emportées.
- Voyager avec des **appareils dédiés**, **chiffrés** et **à jour** (2FA partout).
- Privilégier **4G/5G** + **VPN d'entreprise conforme** ; éviter les Wi-Fi publics.
- Règles d'usage en mobilité : **zéro périphérique inconnu**, prudence sociale.
- **Plan d'incident** (perte/saisie/compromission) + contacts IT/juridique/consulat.
- Au retour : **rotation des secrets**, **audit des appareils**, **RETEX**.

2. Mode d'emploi

- Cette check-list est un **superset**. Coche uniquement ce qui s'applique.
- Complète les **variables pays** (légalité VPN/chiffrement, pouvoirs de fouille, etc.).
- Conserve la page **Contacts & Escalade** jointe et remplis-la avant départ.

3. Check-list opérationnelle universelle

A. Gouvernance & organisation

- ☐ Identifier les “crown jewels” et les données interdites de sortie.
- ☐ Désigner un référent sécurité voyage (24/7) + suppléant.
- ☐ Définir la chaîne d’alerte (IT, juridique, RH, direction).
- ☐ Mettre à jour la politique mobilité (VPN, stockage, messageries autorisées).
- ☐ Créer des comptes temporaires à privilèges minimaux pour la mission.
- ☐ Établir une matrice de risques par pays et des “lignes rouges” (sujets/outils).
- ☐ Préparer un kit d’incident : procédures courtes, modèles de messages, numéros consulat/assurance.
- ☐ Planifier un contrôle post-mission (audit, réimage si doute).

B. Préparation technique (avant départ)

- ☐ Utiliser un laptop et un smartphone dédiés (sans données perso).
- ☐ Activer chiffrement intégral, boot sécurisé, PIN/mot de passe fort, biométrie (en complément).
- ☐ Mettre à jour OS/firmware/apps ; désinstaller le superflu.
- ☐ Activer 2FA (codes de secours hors ligne).
- ☐ Installer un gestionnaire de mots de passe (coffre préparé avant départ).
- ☐ Désactiver auto-connexion Wi-Fi/Bluetooth/NFC/AirDrop.
- ☐ Activer localisation et effacement à distance (MDM/EMM si possible).
- ☐ Installer et tester le VPN d’entreprise ; prévoir un plan B si VPN interdit.
- ☐ Créer un profil navigateur “voyage” propre ; vider caches et cookies.
- ☐ Marquer physiquement les appareils ; consigner numéros de série + inventaire.
- ☐ Faire une sauvegarde complète hors ligne laissée au siège.
- ☐ Générer des versions “light” des documents (métadonnées nettoyées, watermark si utile).
- ☐ Préparer justificatifs : ordre de mission, hotline IT, note matérielle.

C. Cadre légal et frontières

- ☐ Vérifier lois locales : chiffrement, VPN, export-control, pouvoirs de fouille.
- ☐ Décider avec le juridique : usage (ou non) du VPN et alternative documentée.
- ☐ Préparer un script de réponse en cas de demande d’accès par une autorité.
- ☐ Définir infos non partageables et sujets non discutables en public.
- ☐ Aux contrôles : appareils éteints, en cabine, sous surveillance visuelle.
- ☐ Si rétention/saisie : journaliser faits/interlocuteurs et alerter IT/juridique.

D. OpSec physique et discrétion

- ☐ Garder les appareils sur soi ; pas en chambre d'hôtel ni en salle de réunion.
- ☐ Utiliser un filtre de confidentialité d'écran.
- ☐ Pas d'infos sensibles dans le coffre d'hôtel.
- ☐ Aucune discussion sensible en lieux publics (hall, taxi, restaurant, avion).
- ☐ Pas d'annonce de déplacements en temps réel sur réseaux sociaux.
- ☐ Sac discret (sans logo), badges anonymisés.
- ☐ Power-bank personnelle ; éviter bornes de recharge USB publiques.
- ☐ Retirer la SIM si appareil laissé un instant ou contrôle imminent.

E. Réseaux et communications

- ☐ Prioriser partage 4G/5G ; éviter Wi-Fi publics pour opérations sensibles.
- ☐ Si Wi-Fi public imposé : VPN + périmètre limité.
- ☐ Purger réseaux mémorisés ; désactiver radios hors usage.
- ☐ Utiliser messageries chiffrées approuvées ; pas d'apps non autorisées.
- ☐ Limiter visioconférences aux plateformes approuvées (enregistrement off par défaut).
- ☐ Pas d'appels sensibles sur lignes hôtelières/softphones non approuvés.
- ☐ Cloisonner pro/perso (profils séparés ; pas de BYOD non géré).
- ☐ DNS/DoH seulement via configuration approuvée.

F. Périphériques et ports

- ☐ Refuser tout périphérique offert (USB, adaptateurs, cartes SD).
- ☐ Utiliser uniquement ses chargeurs et câbles ; adaptateur USB "power-only" recommandé.
- ☐ Autorun désactivé ; analyser tout média amovible avant usage.
- ☐ Ne jamais brancher ses appareils sur des PC publics (centres d'affaires, cybercafés).

G. Données et applications

- ☐ Chiffrer les fichiers sensibles ; privilégier accès à la demande (lien sécurisé).
- ☐ Pas de stores/applications non officiels ; éviter apps locales non indispensables.
- ☐ Nettoyer métadonnées (auteur, GPS, historique) avant partage.
- ☐ Politique de rétention courte (conversations/fichiers temporaires).
- ☐ Cloisonner projets/clients (espaces dédiés, droits minimaux, liens temporisés).
- ☐ Documenter toute exception locale (outil imposé) et son périmètre d'usage.

H. Ingénierie sociale

- ☐ Refuser invitations/cadeaux non essentiels ; prudence "rencontres fortuites".
- ☐ Vérifier l'identité et le besoin d'en connaître avant tout partage.

- Éviter QR codes inconnus ; préférer URL tapée ou source officielle.
- Revalider par un canal distinct toute demande inhabituelle/urgente.

I. Gestion d'incident (pendant la mission)

- Perte/vol : verrouillage + effacement à distance, dépôt si nécessaire, alerte immédiate.
- Saisie/inspection : consigner et contacter IT/juridique ; suspendre accès.
- Compromission suspectée : couper connectivité, isoler appareil, basculer sur device de secours.
- Révoquer immédiatement sessions, tokens, clés ; forcer réauthentification.
- Notifier clients/partenaires selon protocole.
- Ouvrir un ticket et horodater toutes les actions.

J. Retour et RETEX

- Changer tous les mots de passe, régénérer clés/tokens, invalider appareils de confiance.
- Examiner journaux d'accès (SIEM/MDM/EDR) ; rechercher anomalies.
- Scanner les appareils (anti-malware/EDR) ; forensic si doute.
- Réimage propre avant réintégration au SI si nécessaire.
- Purger caches, cookies, historiques, fichiers temporaires.
- Rapatrier données via canal sécurisé puis supprimer toute copie locale résiduelle.
- Tenir un RETEX (réussites, écarts, améliorations) et mettre à jour politique et kits.
- Briefer l'équipe sur les tentatives d'approche/ingénierie sociale rencontrées.

4. Variables à adapter par pays (à compléter)

- Légalité/conditions d'usage VPN : …
- Régime chiffrement (transport/stockage) : …
- Pouvoirs de fouille aux frontières (appareils, mots de passe) : …
- Plateformes/services déconseillés/interdits : …
- Risque d'ingénierie sociale ciblée (secteurs/acteurs) : …
- Canaux sûrs recommandés (messagerie, conférence) : …
- Contacts locaux (consulat, CERT, assureur) : …

5. Contacts et escalade (à remplir avant départ)

Référent sécurité (24/7) : Nom / Tél. / Email
Juridique : Nom / Tél. / Email
IT Helpdesk : Nom / Tél. / Email
Direction/Client sponsor : Nom / Tél. / Email

Assistance/Assureur : Police / N° urgence
Ambassade/Consulat : Adresse / Tél. / Email

6. Références génériques (pour cadrage interne)

- ANSSI – Passeport de conseils aux voyageurs
- CISA (US) – International Travel
- NCSC (UK) – Travel Security Guidance
- NCSC Suisse – Voyager en toute sécurité
- ACSC (AU) – Travelling overseas

Besoin d'un accompagnement :

Contacter nous

expert@crisehelp.fr