

CONSIGNES DE CYBERSÉCURITÉ POUR LES VOYAGES OFFICIELS À L'ÉTRANGER



AVANT LE VOYAGE

- Informer le COCD de son déplacement prévu.
- Vérifier les lois locales du pays visité sur la technologie et la vie privée ainsi que les obligations en cas de fouille.
- Utiliser uniquement la carte SIM fournie par le COCD.
- Ne pas modifier les réglages d'origine de l'appareil.
- Choisir un NIP d'au moins six (6) chiffres ou un mot de passe robuste pour déverrouiller l'appareil.
- Accéder aux données organisationnelles uniquement au moyen d'un navigateur Web.
- Apporter les câbles, les chargeurs et les adaptateurs nécessaires.



PENDANT LE VOYAGE

- Utiliser exclusivement l'appareil fourni par le COCD.
- Garder l'appareil sur soi, jamais dans les bagages enregistrés.
- Garder la liste des contacts d'urgence fournie par le COCD.
- Se déconnecter et effacer l'historique du navigateur, surtout avant un passage frontalier.
- Éteindre l'appareil lorsqu'il n'est pas utilisé, surtout avant un passage frontalier. L'allumer ou le déverrouiller uniquement sur demande des autorités compétentes.
- Signaler immédiatement au COCD tout vol, toute perte, toute fouille ou toute compromission de l'appareil.
- Se connecter uniquement à des réseaux Wi-Fi fiables et vérifier que le réseau privé virtuel (VPN) fonctionne.
- Éviter toute connexion Bluetooth à un véhicule de location.
- Utiliser uniquement les plateformes de communication approuvées par l'organisation.
- Ne pas numériser de codes QR ou visiter de sites Web inconnus.
- Ne pas installer d'applications lourdes et limiter la permission de géolocalisation. En cas de doute, vous pouvez vous référer au COCD de votre organisation.
- Utiliser uniquement ses propres accessoires électroniques, branchés à une prise électrique.
- Faire preuve de vigilance par rapport à l'utilisation de l'appareil et aux conversations en présence d'inconnus.



APRÈS LE VOYAGE

- Rendre l'appareil au COCD.
- Modifier ses mots de passe et NIP.