**Annexe I à l'instruction administrative ICC/AI/2022/004**

# Liste récapitulative des exigences en matière de sécurité fixées par la Cour pénale internationale

## Exigences en matière de sécurité

### Environnement général

- L'espace de travail doit disposer d'une aération et d'un éclairage adéquats.
- L'espace de travail doit être propre et suffisamment calme ; il doit permettre au fonctionnaire de travailler sans être distrait.
- Les allées, portes et coins doivent être dégagés afin de ne pas gêner le passage.
- L'espace de travail et les aires de passage doivent être libres de tout objet dont la présence ou la chute pourrait provoquer des blessures.
- L'espace de travail doit être équipé d'un extincteur.
- Le numéro d'urgence doit être connu/affiché dans l'espace de travail.
- Une trousse de secours doit être à portée de main et réapprovisionnée au besoin.
- Aucune substance liquide ne doit être présente au sol et ce dernier ne doit pas être glissant ; aucun produit dangereux ou inflammable ne doit se trouver à proximité de l'espace de travail ; et
- Le lieu de télétravail désigné doit être conforme aux mesures de sécurité applicables au domicile dans le lieu d'affectation.

### Électricité/Équipement

- Les appareils électriques situés dans l'espace de travail ne doivent présenter aucun danger connu susceptible de provoquer des blessures physiques (par exemple, câbles ou fils dénudés, détachés ou exposés).

- Le matériel informatique et les prises électriques nécessaires doivent être conformes aux normes de sécurité en vigueur dans le pays.
- Le matériel doit être placé à une hauteur de vision confortable et la chaise ajustée de manière ergonomique.
- Le matériel informatique doit être placé sur un meuble solide, qui est à niveau et correctement entretenu ; il doit être à une hauteur et dans une position permettant de limiter la pression sur les poignets ; et
- Les lignes téléphoniques, les câbles électriques et les rallonges doivent être fixés sous un bureau ou le long de plinthes, et aucun câble ne doit traverser les couloirs ou les aires de passage.

Sécurité

- L'espace de travail doit être équipé d'un détecteur de fumée et d'un détecteur de monoxyde de carbone (CO) en état de marche.
- Lorsqu'ils sont laissés sans surveillance, les documents et le matériel liés à la Cour doivent toujours être conservés en lieu sûr et sous clé.
- Un inventaire détaillé de tous les documents et de tout le matériel liés à la Cour doit être conservé en dehors de l'espace de travail afin que toute perte soit repérée et signalée.

Environnement de travail

La consultation et le traitement d'informations non publiques de la Cour doit se faire dans un environnement de travail remplissant les conditions minimales suivantes :

- Il doit être entièrement situé dans un bâtiment équipé de systèmes de contrôle des accès, où le public n'est pas autorisé (un domicile privé disposant d'une porte d'entrée verrouillée est un environnement acceptable, tandis qu'un restaurant ou un café ne l'est pas) ; et
- Il doit être protégé des oreilles ou des regards indiscrets (par exemple, cloisons de séparation, rideaux ou portes pour empêcher que l'écran d'ordinateur et les informations de la Cour puissent être vus par des personnes non autorisées).

## Gestion des risques et exigences en matière de sécurité de l'information

Les exigences suivantes font partie des mesures essentielles en matière de gestion des risques liés au télétravail. Elles décrivent les comportements et pratiques à suivre (et à éviter), la configuration de sécurité minimale des ordinateurs et de la connexion Internet, ainsi que l'environnement du lieu du télétravail.

Dans le cadre du télétravail, les fonctionnaires sont tenus de respecter l'instruction administrative relative à la Politique de protection des informations de la CPI.

## Sensibilisation à la sécurité de l'information

Le télétravail expose davantage les fonctionnaires aux cybermenaces tout en réduisant leur cyberprotection. Les fonctionnaires demandant à travailler à distance doivent veiller particulièrement à se tenir à jour de l'évolution des cybermenaces.

Les fonctionnaires travaillant à distance doivent tenir à jour leurs connaissances en matière de sécurité de l'information en suivant l'ensemble du programme de sensibilisation offert par la Cour à cet effet, condition sine qua non pour être autorisés à continuer de travailler à distance. Il est à noter que ce programme est proposé de façon continue et non en tant que formation organisée une fois par an.

## Utilisation acceptable

Travaillez de façon sécurisée en n'utilisant que des solutions d'accès à distance et des logiciels approuvés :

- Utilisez uniquement Citrix (ou toute autre solution d'accès à distance approuvée par la Cour) si vous travaillez sur des documents (numériques) de la Cour ;
- Ne travaillez pas sur des fichiers de la Cour en dehors de l'environnement Citrix ou de toute autre solution d'accès à distance approuvée par la Cour ;
- Ne transférez pas de fichiers/données en dehors de l'environnement Citrix ou de toute autre solution d'accès à distance approuvée par la Cour (n'envoyez pas de fichiers sous forme de pièce jointe à une adresse électronique privée) ;
- Ne copiez pas de fichiers depuis Citrix ou toute autre solution d'accès à distance approuvée par la Cour sur le disque dur de votre ordinateur ou sur un service de stockage dématérialisé (« le cloud ») ;
- N'imprimez pas de documents de la Cour lorsque vous travaillez à distance. Tous les documents doivent être imprimés au siège de la Cour ou dans un bureau de pays ; et
- Ne copiez pas et n'échangez pas de fichiers provenant d'ordinateurs de la Cour pour les utiliser en dehors de ses locaux (ne copiez pas de fichiers sur une clé USB, n'envoyez pas de fichiers sur le cloud, n'utilisez pas de services de partage de fichiers et n'envoyez pas de fichiers par courrier électronique).

Communiquez avec vos collègues de la Cour de manière sécurisée, en prenant soin d'éviter les sujets sensibles :

- Ne parlez pas au téléphone (ligne fixe ou mobile) de questions sensibles ou concernant les activités de la Cour ;
- L'utilisation de services de messagerie approuvés, tels que Teams, WhatsApp, Signal, FaceTime et Webex, est autorisée pour les appels audio, l'échange de messages et/ou la vidéoconférence (mais veillez dans la mesure du possible à éviter de parler de sujets sensibles). Assurez-vous que vous communiquez avec le bon interlocuteur et veillez bien à ce que personne ne se trouve derrière vous lorsque vous êtes en communication vidéo.

Soyez vigilant et signalez tout incident potentiel en matière de sécurité :

- Tout incident lié à la sécurité des informations de la Cour doit être signalé au plus vite à votre supérieur hiérarchique, au Service d'assistance informatique ou à l'Unité de la sécurité des informations (+31 70 515 8888 ou +31 70 515 8585).

## Configuration de sécurité minimale pour les ordinateurs et la connexion Internet

Dans l'environnement Citrix ou toute solution d'accès à distance approuvée par la Cour, la consultation d'informations de la Cour doit se faire sur un ordinateur remplissant les conditions minimales suivantes en matière de sécurité :

- L'ordinateur doit être équipé de Windows 10 (ou version ultérieure), MacOS 10.14 (Mojave) ou version ultérieure, ou Chrome OS 93, version stable, ou ultérieure ;
- Le système d'exploitation doit être mis à jour régulièrement à l'aide des correctifs de sécurité recommandés par le fournisseur ;
- L'ordinateur doit être équipé d'un pare-feu local configuré pour empêcher tout accès à l'ordinateur depuis le réseau local et Internet ;
- L'ordinateur doit être équipé d'un logiciel antivirus activé disponible dans le commerce, dont les signatures n'ont pas plus de 14 jours ; une analyse complète du système doit être réalisée au moins tous les 30 jours ;
- L'ordinateur doit disposer d'une fenêtre de connexion obligatoire exigeant au minimum un nom d'utilisateur et un mot de passe ;
- Le compte utilisateur utilisé pour travailler sur des documents de la Cour (et, dans l'idéal, l'ordinateur lui-même) ne doit pas être utilisé par les autres membres de la famille ; et

- Le verrouillage de l'écran de l'ordinateur (ou équivalent) doit être activé automatiquement en l'absence du fonctionnaire.

La connexion Internet doit remplir les conditions minimales suivantes en matière de sécurité :

- Si la connexion est fournie par une société commerciale ou une organisation similaire :
    - La connexion Internet (WiFi) doit être identifiable comme appartenant à ladite organisation et ne doit être accessible que dans des zones se trouvant raisonnablement sous le contrôle de cette dernière (par exemple, le réseau Wifi de la CPI ne devrait raisonnablement être accessible que dans le bâtiment de la Cour ou à proximité immédiate de celui-ci. Si l'on vous propose de vous connecter à ce réseau en dehors de ce périmètre, il s'agit très vraisemblablement d'une activité malveillante) ;
- Si la connexion Internet est gérée par l'intermédiaire d'une personne privée (par exemple, un réseau à domicile ou une clé 3G ou 4G) :
    - Le réseau/appareil proposant la connexion Internet doit exiger un mot de passe,
    - Le routeur Internet (ou routeur WiFi) doit être configuré à l'aide d'un mot de passe administrateur renforcé afin d'empêcher les accès non autorisés et les changements intempestifs des réglages (les mots de passe par défaut/configurés en usine doivent être modifiés),
    - Toute clé 3G ou 4G doit aussi être configurée à l'aide d'un mot de passe administrateur renforcé.