Annex I to Administrative Instruction ICC/AI/2022/004

The International Criminal Court's Security and Safety Checklist

Safety Controls

General Environment

- The workspace area has adequate lighting and ventilation;
- The workspace is kept clean and reasonably quiet and free from distractions;
- Aisles, doorways, and corners are free from obstructions so to permit movement;
- There are no items near the workspace or areas of movement that could fall against/on and injure oneself;
- There is a fire extinguisher in the workspace;
- The emergency number is known/posted at the workspace;
- A first aid kit is easily accessible and replenished, as needed;
- There are no fluids on the floor nor is the floor slippery and there are no hazardous or inflammable materials in proximity to the workspace; and
- The specified remote workplace in the field meets the Residential Security Measures (RSM) standards specific to the duty station.

Electricity/Equipment

- All electrical equipment at the workspace is free from recognized hazards that would cause physical harm (e.g. frayed wires, bare conductors, loose or exposed wires);
- Computer equipment and necessary electrical outlets are compliant with electrical safety standards of the country of use;
- The equipment is placed at a comfortable height for viewing, and the seating arrangement is ergonomically adjusted;

- The computer equipment is on a sturdy, level, and well-maintained piece of furniture, at a height and in a position that does not cause wrist strain; and
- Phone lines, electrical cords, and extension wires are secured underneath a desk or along baseboards and there are no cables across hallways or areas of movement.

Safety and Security

- There is a working smoke and CO detector in the workspace;
- Any material or equipment related to the Court is secure at all times and locked when unattended; and
- A detailed inventory of all material and equipment related to the Court is maintained outside of the remote place of work in order to identify and be able to report any loss of material or equipment.

Working Environment

The working environment where access to (and processing of) any non-public Court information is to take place must meet the following minimum standards:

- It is wholly contained in an access-controlled building, where the public are not admitted (a private house with a locked front door is acceptable, a restaurant or café is unacceptable); and
- It provides protection against being overseen or overheard (i.e. suitable screens / curtains / doors are used in the working environment to prevent the computer screen and any Court information from being seen by unauthorised persons).

Risk Management and Information Security Controls

The following controls form the critical risk-management measures applicable for working remotely. They describe the acceptable (and unacceptable) behaviours and practices to be followed, and also describe the minimum acceptable security standards to be applied to the computer and Internet connection, and the working environment at the remote working location.

While working remotely, staff members shall adhere to, and comply with, the Administrative Instruction on ICC Information Protection Policy.

Information Security Awareness

Working from a remote location exposes the staff member to increased cyber-threats coupled with decreased cyber-security protection. Staff members that request to work remotely must pay particular attention to the maintenance of their awareness of cyber-threats.

Staff members working remotely shall maintain their awareness by staying current with the latest information security awareness training offered by the Court. A condition of continuing permission to work remotely is the completion of all provided information security awareness training. Note that such training is offered on a continuing basis, not as a single annual course.

Acceptable Use

Work securely using only approved remote access solutions and software.

- Use only Citrix (or any other Court-approved remote access solution) for all remote working on Court (digital) information;
- Do not work on Court files outside Citrix or any other Court-approved remote access solution;
- Do not transfer files / data outside the Citrix environment or any other Court-approved remote access solution (i.e. do not send files as attachments to a private email address);
- Do not copy files from Citrix or any other Court-approved remote access solution to your local computer hard disk or cloud storage service;
- Do not print Court documents when working remotely. All documents must be printed at HQ or a Country Office; and
- Do not copy or exchange files from Court computers to use outside the Court (i.e. do not copy files to USB, do not send files to Cloud storage applications, do not use file sharing services, and do not send files via email).

Communicate with Court colleagues securely, and minimise the sensitivity of communication.

- Do not discuss any sensitive or operational matters when using a regular telephone (landline or mobile).
- It is acceptable to use a Court-approved messaging service such as Teams, WhatsApp, Signal, FaceTime and Webex for voice calls, messaging and/or video-conferencing (but avoid especially sensitive subjects as far as possible). Ensure you are communicating with the intended recipient, and be cautious of the view behind you when using video!

Be alert for and report any potential security incidents.

- Report any security incidents involving Court information to your supervisor, the IT Service desk or the Information Security Unit as soon as possible. (+31 70 515 8888 or +31 70 515 8585).

Minimum acceptable security configuration of Computer and Internet

The computer being used with Citrix or any other Court-approved remote access solution to access Court information must meet at least the following minimum security standards:

- It uses Windows 10 (or later), MacOS 10.14 (Mojave) or later, or Chrome OS stable version 93 or later;
- The operating system is regularly maintained with vendor-recommended security patches;
- The computer has a local firewall enabled, configured to prevent access to the computer from the local network and from the Internet;
- The computer has commercial anti-virus software installed and enabled, updated with signatures no older than 14 days. A full system scan has been completed within the past 30 days and is regularly repeated;
- The computer has a mandatory login screen, requiring a minimum of a username and password;
- The user logion account used for Court purposes (and ideally the entire computer) is not shared with other household members, and
- The computer screen lock (or equivalent) is active / engaged whenever the staff member is not present.

The Internet connection to be used by the computer meets the following minimum security standards:

- If the Internet connection is managed by a commercial company or similar organisation:
    - The Internet connection (commonly WiFi) identifies itself as belonging to the organisation, and is accessible in areas that are reasonably within the expected control of that organisation (e.g. The ICC WiFi network should reasonably only be accessible within or in very close proximity to the ICC building. If it were offered elsewhere, this would represent a clear indication of a threat actor).
- If the Internet connection is managed by a private individual (e.g. via a home network or 3G / 4G dongle):
    - The network / device offering the Internet connection requires a password to join / use.

- The Internet router (commonly the WiFi router) is configured with a strong administrative password to prevent unauthorised access and prevent uncontrolled configuration changes. Default / factory-set passwords must be changed.
- A 3G / 4G dongle is similarly configured with a strong administrative password.