Annex to Administrative Instruction

Ref. ICC/AI/2019/002

Date: 11 February 2019

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 someone and cause injury;
- 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 workplace so that any loss of material or equipment can be identified and reported.

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).
- 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 unauthorized persons).

Risk Management and Information Security Controls

The following controls form the critical risk-management measures applicable for working remotely. They describe the acceptable behaviours and practices to be followed (along with unacceptable practices and behaviour), 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 ICC/AI/2007/001 ("*ICC Information Protection Policy*").

Acceptable Use

Use only Citrix (or BlackBerry Good if using a smartphone) for all remote working on Court (digital) information.

- Do not work on Court files outside Citrix;
- Do not transfer files/data outside the Citrix environment (e.g. do not send files as attachments to a private email address);
- Do not copy files from Citrix to your local computer hard disk or cloud storage service;
- Do not print Court documents when working remotely. All documents must be printed in the Court's premises in the duty station; 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, and do not send files via email).

Communicate with Court colleagues securely, and keep all communication non-sensitive.

- Do not discuss any sensitive or operational matters when using a telephone (landline or mobile).

- It is OK to use WhatsApp, Signal, FaceTime or Cisco Webex for voice calls, messaging and/or video-conferencing (keep the calls/messages short and non-sensitive). 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 incidents involving Court information to your supervisor, the IT Service desk or Information Security Unit as soon as possible. (070 515 8888 or 070 515 8585)

Minimum acceptable security configuration of Computer and Internet

The computer being used with Citrix to access and process Court information meets the following minimum security standards:

- It uses Windows 7 (or later) or Mac OS X 10.10 Yosemite (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; and
- The computer screen lock (or equivalent) is on whenever the staff member is not present.

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

- If the Internet connection is provided by a commercial or similar organization:
    - The Internet connection (commonly WiFi) identifies itself as belonging to the organization, and is accessible in areas that are reasonably within the expected control of that organization (e.g. The ICC WiFi network should reasonably only be accessible within the ICC building. If it were offered elsewhere, this would represent a clear indication of a threat actor).
- If the Internet connection is provided via a private individual (e.g. 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 unauthorized 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.