INFORMATION SECURITY AND CONFIDENTIALITY FOR MECHANISM STAFF[1] WORKING REMOTELY DURING THE OUTBREAK OF COVID-19

1. During this time, as most Mechanism staff members are working remotely, it is important to step up awareness of digital and information security. This document has been created to remind staff of their responsibilities for information security and confidentiality when working remotely.

2. While engaged at the Mechanism, staff are given access to confidential and strictly confidential.[2] Access to this type of information is normally defined by the information manager of a particular area of work, usually the Section Chief or direct supervisor and the functions of a staff member's post. This is based on the principles of "Need to Know" and "Need to Hold".

3. In this context, information is defined as any resource, knowledge, documentation, papers, materials, items, or anything whatsoever in possession or control of a staff member as a direct or indirect consequence of engagement by the Mechanism. This includes all material in whatever format, both physical and electronic.

4. The protection of our information asset remains the personal responsibility of each individual. The basic principle of "Need to Know" and "Need to Hold" remains in place no matter where staff are working. The objectives of information security do not change when working away from the office. Indeed, when working from home or elsewhere they are more important.

5. In this respect, staff are reminded of their obligation to protect all Mechanism information and not to communicate in any way confidential or strictly confidential information to any person who is not a staff member of the Mechanism or to any other person who is not authorised to have such information. Always be aware of your surroundings both inside the Mechanism premises and elsewhere: who else is present? Should this matter be discussed in front of them?

6. The following measures should be applied by all staff working remotely:

   a. Don't draw attention to the fact that you are working on official information at home.

   b. Make sure that your equipment is in a safe location at all times such as in a private room at home, and locked away when not in use. Protect access to your equipment and information resources with a strong password[3] and/or a two-factor authentication. Do not save your log-in credentials in your browser.

[1] The term "Mechanism staff" refers to all those engaged by the Mechanism in any capacity to facilitate its core mandate. This encompasses staff, judges, interns, contractors, along with any other person.
[2] Please see ST/SGB/2007/6, "Information sensitivity, classification and handling", which defines classification levels for sensitive information.
[3] The key aspects of a "strong password" are length (at least 10 characters); a mix of letters (upper and lower case), numbers, and symbols, no ties to your personal information, and no dictionary words.

c. Keep your computer up to date.

d. Check from time to time if there are updates on the operating system and software available. Ensure that all personal devices are protected with latest security patches. Optionally, if available, you can use a VPN to increase your online security and privacy.

e. Connect to the internet via secure networks. Do not use open/free networks. The use of public facilities, such as (internet) cafes, shops, libraries, restaurants, airports, are not approved.

f. Protect your passwords (do not write them down, do not share them with anybody), and (United Nations) software, equipment, facilities and systems from unauthorized access and disclosure. Do not furnish your login credentials or authentication devices to anyone. Mechanism officials and ITSS will never ask for your passwords, and anyone who asks for them should be treated with caution.

g. Protect sensitive files and documents from unauthorized access and disclosure by keeping them out of sight from un-authorised persons during working hours and furthermore locked away when not in use.

h. Only the minimum amount of sensitive material should be held at the remote workplace and for the minimum amount of time. Staff are to review what information they hold at home and reduce it to the absolute minimum needed to effectively work. Such holding should be reviewed on a weekly basis and non-essential documents should be returned to the office.

i. When transporting official documents to home, care must be taken to ensure that they cannot be seen by others, and that they are protected from compromise, loss or theft, both while in public and at home.

j. If you are working on an official laptop then it is to be restricted to work use only.

k. If you are using a private computer, ensure that you can identify any official content on the device and arrange for its deletion immediately when it is no longer of use.

l. Under no circumstances should a computer being used to access official resources be left unattended without being disconnected from the Mechanism server.

m. If you have confidential/strictly confidential information on an electronic device, that device should be treated as confidential/strictly confidential. For example, if there is a confidential document on a memory stick, the memory stick itself needs to be protected in the same manner as the printed document. This includes any back-up copies held on memory sticks etc.

n. Confidential and strictly confidential information should not be sent via private e-mail. Staff will communicate securely with team members on sensitive matters only via UN email accounts. This should preferably be done inside the virtual remote connection to avoid downloaded files to remain on the download folder of private devices. Logging out of the Remote Session automatically erases the downloaded files from the download folder. Secure applications approved by the UN such as Microsoft Teams may be used for voice/video communication but should not be used to circulate confidential and strictly confidential documents.

o. Frequently delete your downloading folder if using webmail outside of the remote connection. When attachments to emails are opened in webmail, the files get automatically saved on the device, usually in "downloads." Those files remain on your computer when you close your browser, when you log out of webmail and when you turn off your device, even if you did not save them. This creates a security risk.

p. Telephones, both landline and mobile are not secure and confidential and strictly confidential information should not be discussed on them.

q. All official papers and other materials that are considered as waste must be disposed of by returning them to the office for destruction.

r. When not being worked on, all official documents should be locked away. At the end of any working period, staff are to log out of any remote work applications and ensure that all work product and documents are secured, both physical and electronic.

s. Be careful with any email from sources outside the Mechanism referencing the Corona virus/COVID-19, as these may be phishing attempts or scams. In case of doubt regarding the legitimacy of an email, contact the Security and Safety Section or ITSS.

t. Be suspicious of any email asking to check or renew your credentials even if it seems to come from a trusted source. Please try to verify the authenticity of the request through other means, do not click on suspicious links or open any suspicious attachments.

u. Be suspicious of email from people you don't know, especially if they ask to connect to links or open files, or that create a sense of urgency. Also be suspicious of emails which appear to come from people you know, but which are asking for unusual things.

7. Any loss or compromise of information regardless of cause is to be reported to supervisors immediately. Any security incident should be immediately reported to the Security and Safety Section.

8. Workgroups may further supplement these instructions where their unique circumstances require additional or specific protective measures.