Secretariat Security Standards for the Use of the Commission Data

March 2018

1. The following features are the mandatory requirements for the Secretariat's staff use of the Commission data:

   a) Staff will be provided with only the keys, passwords and combinations required for them to undertake their direct work functions.

   b) A key register is maintained by the Executive Secretary as well as secure storage of spare keys.

   c) Staff are responsible for the integrity of their workplace security and common entry and exit doors. Office doors shall be locked after hours when staff are away from their workplaces as well as windows. Doors other than the main entry door should be locked when not in immediate use.

   d) Staff are to check their rooms and the premises as they leave the main office or any of the other buildings to ensure all windows and doors are properly secured. The Executive Secretary will ensure that special checks at the end of each work day will be undertaken.

   e) Keys, passwords and combinations are to be kept secure.

   f) Visitors to the SPRFMO Secretariat are required to register upon access to the premises. Visitors, including family members, are not to be permitted to move around the building unescorted.

   g) Each staff user shall be assigned a unique user identification and associated password. Each time the user logs on to the system he/she has to provide the correct password. Even when successfully logged on, the staff user shall only have access to those functions and data that he/she is configured to have access to.

   h) System security issues/events must be auditable by a third party at any time at the request of the Commission.

   i) The Secretariat should develop an administrative procedure for the purposes of implementing these requirements.

2. The Secretariat, in consultation with the CTC Chair, shall develop internal electronic data and communication security procedures at the latest one month after the date established in paragraph 1 of CMM06-2018 based on the following key guidelines:

   a) Establishing adequate disaster recovery plan and procedures.

   b) Prevention of network compromise:

      i. Only authorised staff at the Secretariat have access to the corporate network with "strong password" policy in place.

      ii. All corporate servers protected by proven firewall, antivirus and anti-spam solutions with real-time update policies activated. All network devices protected by anti-virus with live electronic updates.

      iii. Logs of key software updates, mail protection (anti-spam), anti-virus, Internet and network events, together with special event alert monitors allow administrators to address any problem issues before they happen.

iv. Appropriate service level agreements (SLAs) are in place for outsourced support of critical systems and applications or otherwise foreseen in the contract with the Secretariat's IT service providers.

c) Prevention of data compromise:

i. Procedures to define "acceptable mobile device for SPRFMO use" and restriction.

ii. Automated procedures to keep all approved software "up-to-date".

iii. Staff training on prevention of data compromise.

d) Prevention of data loss:

i. An enterprise backup and recovery solution is in place with full backups of business data run daily, Monday to Friday, and stored offsite.

ii. Staff training on storage of important business data in public folders or shared folders which get backed up.