

No. 19-1/2024-AS-IV
Government of India
Ministry of Communications
Department of Telecommunications
Access Services Wing
Sanchar Bhawan, 20, Ashoka Road, New Delhi-110001

Date: 16.01.2025

Office Memorandum

Subject: - Standard Operating Procedure for traceability of users of 'In Flight and Maritime Connectivity' (IFMC) services

This is in reference to Standard Operating Procedure for traceability of users of In Flight and Maritime Connectivity (IFMC) services issued by Department of Telecommunications (DoT) on 11th November 2024. In this regard, consultation has been carried out with all the stakeholders including IFMC service providers, Domestic Airlines, International Airlines, International IFC service providers, DGCA and LEAs. Based on the feedback, the procedure has been revised in the present document. The earlier procedure dated 11th November 2024 stands superseded.

1. Background

1.1. IFMC service authorizations are being issued by Department of Telecommunications (DoT) under the Flight and Maritime Connectivity Rules, 2018. The IFMC service provider establishes, maintains and operates communication services to provide wireless voice or data on ships within Indian territorial waters and on aircraft within or above India or Indian territorial waters.

1.2. The IFMC authorization requires that the IFMC service provider, before providing IFMC service to its subscribers, shall ensure their traceable identity as and when required by the Government. Thus, the IFMC service provider must provide traceable identity of their users who are availing wireless voice or data services onboard an aircraft or ship vessel.

2. Objective

The procedure, outlined below, aims to identify the passenger who has operated the internet/voice session by linking the device/session parameters with passenger information.

3. Procedure

3.1 Before permitting the use of IFMC services on-board an aircraft/ship vessel, the credentials of the passenger may be captured and authenticated.

- 3.2 The credentials used shall uniquely determine the passenger and should be selected in a manner to make it difficult for any possible impersonation.
- 3.3 Validated credentials of the user may be mapped with the MAC Address/IMEI/Other device identification number of the user device.
- 3.4 The authentication process on-board aims to provide for irrefutable linkage between the IFMC session and the user identity.
- 3.5 In the event of requirement of details of session user from Law Enforcement Agencies(LEAs), the IFMC service providers shall collect the information from Aircraft/Ship vessel operators and provide it to LEAs. However, in case Aircraft/Ship vessel operators does not want to share the data with IFMC Service Providers, the requested information may be directly provided by the Aircraft/Ship vessel operators to LEAs.
- 3.6 The information supplied to LEAs, upon request, shall, inter-alia, contain the PNR details and user identity related to the passenger.
- 3.7 Further, IFMC service providers shall ensure, depending upon feasibility, that the WiFi Hotspot tethering facility is not allowed on the user device which is using IFMC services.
- 4** The above procedure is applicable on domestic as well as international aircraft routes and for domestic as well as foreign passengers.
- 5** All IFMC Service Providers are requested to ensure that their agreements with Partner Licensee as well as Aircraft/Ship vessel operator have requisite provisions to ensure compliance as detailed above.
- 6.** The procedure will be effective from 01st April 2025.

Director (AS-II)
Tele No. 23372370

To
All IFMC Service Providers

Copy to :

1. Secretary, Ministry of Civil Aviation
2. Special Secretary (IS), MHA
3. DG Civil Aviation
4. DG Shipping