7 PROTECTION AND RETENTION OF FDAP DATA

7.1 OVERALL APPROACH

The main objective of FDA program is to improve safety by identifying trends, not individual acts. Therefore, data obtained from FDA will not be used primarily as the basis to take disciplinary action against the pilot. The data will only be used for Accident prevention purposes and the information shall not be used in a way different from the purposes for which it was collected.

Onboard the aircraft, the electronically derived recorded data can contain commercially and personally sensitive information. As such, it is important that access to it is carefully controlled and limited to those people with a need to be aware of the data contents. The CVR and FDR are protected from any inappropriate use such as public disclosure or the disclosure of crew information.

FDAP generates enormous amount of data, and it is the responsibility of FDAP manager to ensure the proper-

1. Access, Retention and Archiving
2. Security
3. Retrieval

Data generated through FDAP program is confidential in nature hence proper safeguards shall be implemented to avoid any unauthorized access to the data.

7.2 DATA STORAGE, RETENTION AND DE-IDENTIFICATION POLICY

In Riyadh Air, all flight data and records are stored on company servers with access restrictions. Access matrix to these servers will be as per table:

User	Server / Software	Data / Access Level	Purpose
Maintenance Personnel		Raw Data	Upload of Downloaded Data (QAR/FDR and CVR)
FDM Cell		Raw, Processed Data, FDM Records, Reports and CVR Raw, processed Data	For data processing, analysis, and grading.
VP- Corporate Safety, Security and Environment/Director Corporate Safety/Flight Data Specialist		Processed Data, FDM Records and Reports	For data analysis and evaluation
Individual Flight Crew		Individual Reports	Self-Analysis

Table 3 Data Access Restriction to Servers

7.3 PROCEDURES FOR IMPLEMENTING AND AUDITING SECURITY MECHANISMS OF DATA

1. The Flight Data Monitoring Program with all flight data readout facility is managed by the Safety Office.

2. Flight data is downloaded from secured company FTP servers and raw data is stored on company servers. The processed data by Software also stores and archives data in secured company servers.

3. Safety Insight Software is a web-based software and dedicated Safety FDM team members access this as per RXI IT security policy.

4. The access to Safety Insight is restricted to dedicated FDM team members and the password is shared with only FDAP team members.

5. The FDAP reports and database and other extracted data from the Safety Insight software is stored in a shared drive-in dedicated folder which is restricted to only Safety-FDAP team members.

6. The access to the servers is restricted through company IT security infrastructure and governed by the IT security policy. For any data shared with external service provider or agency, non-disclosure agreement is signed as per IT security policy.

7. The above policies and processes ensure FDAP data remains protected from unauthorized access and use.

8. With the advancement of technologies (hardware/software), the data management policies will be reviewed, and necessary changes will be introduced in consultation with the digital team/GE team as and when required to ensure safe and secure access to data and improve data management methods and procedures.