2 DATA PROTECTION AND LEGAL AGREEMENTS

2.1 CONFIDENTIALITY AGREEMENT/POLICY

FDAP generates enormous amount of data, and it is the responsibility of Flight Data Specialist under supervision of the VPCSSE to ensure the proper-

1. Access, which is restricted to authorized personnel, ensuring that only individuals with a legitimate need can retrieve or interact with the data.
2. Retention, to manage the life cycle of the FDAP data and data will be retained as per the organization policy.
3. Archiving, Overseeing the archiving process to ensure that historical FDAP data is stored securely and is readily available when needed. Proper indexing and categorization facilitate efficient retrieval.
4. Security, with the help of the IT department, will be ensured.
5. Retrieval, retrieving FDAP data when required for safety analysis, operational improvement, or other authorized purposes.

Data generated through the FDA program is confidential in nature and the integrity of FDA program rests upon protection of the FDAP data. Any disclosure of data that reveals flight crew member identity for purposes other than safety management, can compromise the voluntary provision of safety data, thereby compromising flight safety. Therefore, FDAP data will be provided in a de-identified manner with the permission of the VPCSSE.

The data access and security policy restrict access to FDAP information to authorized persons. In addition, when data access is required for airworthiness and maintenance purposes, troubleshooting and rectification through FDR Readout, the same shall be provided by Safety Office in a de-identified manner.

2.2 WITHDRAWAL OF CONFIDENTIALITY

In the event of accidents or serious incidents requiring external competent authority investigation, the investigative process takes precedence over the routine requirements of the Flight Data Analysis (FDA) program. During such occurrences, the following procedures and considerations will be in effect:

2.2.1 Retention of FDAP Data

1. Accidents and serious incidents will be prioritized for investigation and the associated Flight Data Recorder (FDR) data will be retained as a crucial element of the investigative process.
2. Recognizing that the retention and use of FDR data for investigation purposes may fall outside the scope of de-identification agreements.
3. Understanding that in the interest of a thorough investigation, the data may need to be preserved in its original, non-de-identified state.

2.2.2 Coordination with Investigative Authority

1. Collaborating closely with relevant aviation authorities, investigative bodies and any other stakeholders involved in the post-accident or incident investigation.
2. Complying with legal and regulatory obligations related to the retention and sharing of FDR data for investigative purposes.
3. Acknowledging that during the investigation of accidents or serious incidents, the standard de-identification protocols may be suspended.
4. Ensuring that the suspension is strictly limited to the period required for the investigation and is in accordance with legal and regulatory obligations.

2.2.3 Post-Investigation Procedure:

1. After the conclusion of the investigation, promptly resuming the standard de-identification procedures for FDR data as outlined in the Flight Data Monitoring program.
2. Ensuring that any retained data is handled in accordance with legal and regulatory requirements and is appropriately documented.

2.3 DATA PROTECTIVE PROVISIONS AND SECURITY

Data protection and security are treated as paramount concerns, reflecting Riyadh Air's commitment to safeguarding sensitive information. Provisions are in place to balance the accessibility of data for authorized personnel with robust security measures to prevent unauthorized access.

Under the supervision of VPCSSE, Flight Data specialist is responsible and plays a pivotal role in maintaining the security provisions for FDAP data. Following are the guidelines for the data protection and security:

1. Each individual accessing the FDA program must authenticate using unique credentials, ensuring that only authorized personnel can interact with sensitive flight data.
2. Detailed access logs are maintained to record each instance of login and interaction with the FDA program, providing traceability for accountability.
3. FDAP data is shared in a de-identified manner, with personal identifiable information removed to protect the privacy of flight crew members.
4. When sharing data externally, non-disclosure agreements are established to ensure that the receiving party complies with confidentiality and privacy standards.
5. Flight data is transferred from secured company FTP servers, employing encryption protocols to safeguard data during transit.
6. Raw and processed data are stored on company servers with robust security measures, including firewalls, intrusion detection systems and regular security audits.
7. Archiving of data follows established protocols, ensuring data integrity, accessibility, and compliance with retention policies.
8. Collaboration with the IT security team ensures that the FDA program aligns with the broader IT security infrastructure and policies of the organization.
9. Working closely with IT security teams to implement proactive security measures, including software patches, updates, and vulnerability assessments.

2.4 DATA RECOVERY

Ensures maximum acquisition of the aircraft raw data. As mentioned in the previous chapter, data acquisition is being done in two (2) ways: automatic and manual data retrieval. Nonetheless, the manual data retrieval process also serves as a contingency procedure should the wireless ground link fail, hence, complementing the target retrieval of flight data.

When an incident occurs, a timely and considered judgement is made by the Director of Safety and the DFDR data is required for an investigation. In such cases, the decision to quarantine the DFDR is taken expeditiously considering that the DFDR unit holds up 25 hours of data recording, hence, eliminating the possibility of the data being overwritten.

Validation of processed flight data is performed fervently to eliminate errors and spurious events. This process enables Safety Department to generate more plausible information that is useful in identifying possible threats and / or violations to the safety of the flights.