中華航空 CHINA AIRLINES

China Airlines Information Security and Artificial Intelligence Policy

China Airlines (hereinafter referred to as the "Company") has developed this policy to maintain the security of the Company's information and information assets, prevent unauthorized infringement, keep their confidentiality, integrity, and availability, and comply with applicable laws and regulations.

Scope

The management of information security for the Company's information systems and information business shall be conducted in accordance with the requirements specified in this policy.

Applicable Personnel

All staffs and outsourced supplier personnel shall be familiar with this policy and related management procedures, and implement relevant information security management requirements.

Information Security Objectives

1. Obtain international standard certification, continuously improve the Company's information security management system, and maintain its effectiveness.
2. Implement information assets management and security risk management so that confidential information can be protected during transmission and storage.
3. Prevent information assets from unauthorized tampering and maintain information integrity and cybersecurity through information security protection and control measures.
4. Achieve the continuous availability of information assets operations through the information security incident notification, response, drills and continuous operation plans.
5. Regularly implement information security training to deepen all staff's information security awareness, thereby promoting the establishment of personal responsibility for information security.
6. Emerging technologies shall be incorporated into the information security management system, with corresponding management principles and control requirements established based on risk assessment results. The governance aspects of Artificial Intelligence (AI) applications include:
   (1) Privacy, Data Protection and Cybersecurity:
   Ensure that AI applications process data in accordance with applicable privacy and personal data protection laws and regulations. Adhere to the principle of data minimization. Strengthen cybersecurity controls by the implementation of periodic security measures and auditing activities to prevent unauthorized access, data abuse, and information security threats.
   (2) Fairness and Avoidance of Bias:
   Avoid potential bias or discrimination embedded in AI applications through model design, periodic monitoring and evaluation mechanisms to ensure fair, reasonable, and non-discriminatory outcomes.

(3) Human Oversight and Decision Control:

Keep humans in the loop for critical decisions and allow human intervention for final decisions in AI applications involving flight safety, passenger rights, regulatory compliance, human resources, financial approvals, or other aspects with significant impact.

(4) Transparency and Explainability:

Ensure transparency in AI applications, guaranteeing that the operational principles and decision-making logic of AI possess reasonable explainability.

(5) Accountability and Responsibility:

Establish clear accountability and risk governance responsibilities for AI applications, models, and tools. Information and data-providing units must ensure the accuracy of data used by AI models to support traceability and accountability.

(6) Boundaries of Use and Limitations:

Define clear boundaries and limitations of AI applications. The use of AI for manipulative practices, exploitation of vulnerable individuals, unauthorized biometric surveillance, social scoring, or other activities that violate applicable laws or ethical principles is prohibited.

(7) AI Risk Governance and Ethical Review:

Establish AI risk assessment and classification process, and implement ethical review and approval mechanisms for high-risk AI applications to mitigate potential risks.

(8) Operational Monitoring and Model Management:

Establish continuous monitoring mechanisms for AI models, periodically review model performance, accuracy, and model drift, and implement necessary corrections and optimizations.

Management Review

This policy is adjusted and revised according to relevant laws, regulations and information business needs.

Information Security Management System

The Company has implemented an information security management system in accordance with the ISO 27001 international standard. Core information systems and data networks associated with passenger airline reservations, ticketing, marketing operation processes and airport service have been audited and certified by SGS Taiwan.

Signed:

Chairman **President**

July 18, 2026