



AIDC Safety Email Management Regulation

20260801 Rev A

I. Purpose and Commitment

To implement the Safety Management System (SMS) and establish a "non-punitive" and "confidential" communication environment, Aerospace Industrial Development Corporation (hereinafter referred to as "AIDC") has established the SMS Safety Email (AIDCSMS@ms.aidc.com.tw), which aims to build a "speak-up" culture. We encourage all current employees (including dispatched workers), stakeholders, and third-party partners (including contractors, subcontractors, and suppliers) to proactively report safety hazard risks or suspected misconduct. The Chairman has committed to provide all necessary resources to implement safety improvements and strictly prohibits any form of retaliation against reporters.

II. Scope of Reporting and Content Guidelines

1. **Applicable Domain:** The scope of reporting covers 9 safety-related fields: organization, flight operations, dispatch, maintenance, manufacturing, ground operations, cabin safety, hazardous chemical management (including dangerous goods, toxic and concerned chemical substances), and security.
2. **Event Types:** This includes equipment failures, operational procedure deficiencies, environmental hazards, and near-miss incidents.
3. **Specificity Requirements:** Reports must provide specific details regarding the who, what, when, where, why, and how of the facts. Personal grudges or speculation without concrete evidence will be dismissed.
4. **Timeliness Requirements:** Upon discovering a hazard, reports should be submitted as soon as possible within a specified timeframe (e.g., before the end of the operation) to mitigate risks in a timely manner.

III. Strict Confidentiality and Identity Protection

1. **Dedicated Handling and De-identification:** Emails are designated to be received by dedicated personnel from the "Ethic and Security Department." De-identification processing will be performed immediately upon receipt to ensure the absolute confidentiality of the reporter's identity.
2. **Execution of Exclusive Confidentiality Agreements:** All handling personnel involved in processing the case must sign an exclusive confidentiality agreement to strictly prevent information leakage. Except as

required by law, the identity of the reporter will never be disclosed to any third parties.

3. **Anonymous Reporting Mechanism:** This mailbox accepts anonymous reports. If an anonymous method is used, the handling unit's investigation may be limited due to the inability to conduct follow-up interviews. Consequently, investigation results and improvement status cannot be directly provided to the reporter, and the Ethic and Security Department will promote awareness through public announcements instead.

IV. Just Culture and Incentive Policy

1. **Self-Involved Incidents (Leniency/Immunity Recommendations):** If the reported content involves the reporter's own fault and is "non-intentional," the Ethic and Security Department will recommend leniency or immunity from liability in accordance with the "Just Culture" principles of the SMS Plan.
2. **Exclusion Clauses for Immunity:** If the incident involves intentional violations, major negligence, illegal acts, or alcohol/drug abuse, the aforementioned immunity protection shall not apply.
3. **Third-Party Involved Incidents (Whistleblower Rewards):** Where a reported case involving safety hazards that violate the scope specified in Article II, Section 1 of these Regulations is verified as true, tangible rewards shall be awarded based on the following classifications of the severity/nature of the case:
 - 3.1 Where the informant reports the factual details, proposes substantial improvement measures, and timely prevents a safety disaster, a cash reward of NT\$500 (inclusive) or more shall be granted.
 - 3.2 Where the informant reports the factual details and proposes general/principle recommendations, a cash reward of NT\$200 shall be granted."

V. Handling Procedure and Timeliness

Reported cases will be processed in accordance with the "Handling Procedures for Reported Cases" as follows:

1. **Receipt Acknowledgement:** The Ethic and Security will send an acknowledgement within 3 working days after receiving the report and conduct a case review (including case validation and classification). If the case is determined to be invalid, the reporter will still be notified.
2. **Professional Assignment:** Once a case is validated, the reported content will be forwarded as a confidential document to the SAT leader under the relevant SMG for professional investigation and verification.

3. **Time-Limited Investigation and Follow-Up:** The SAT must report back to the Ethic and Security within a specified timeframe. Depending on the severity level of the case, the responsible unit must report the investigation results within 14 working days. If needed, a one-time extension may be requested from the Director of the accountable SMG, up to a maximum of 28 working days.
4. **Review and Case Closure:** Upon completion of the investigation, the Ethic and Security will conduct a review, and the case can only be closed upon approval.
5. **Results Feedback:** For reporters who provide their names, the Ethic and Security Department will provide feedback on the investigation results.

VI. Data Retention and Legal Validity

1. **Retention Period:** Relevant documents and electronic records shall be retained for at least 5 years for subsequent safety trend analysis or review by competent authorities.
2. **Regulatory Compliance:** Email or system records may serve as legal evidence. The Company will process and protect relevant personal data strictly in accordance with the "Personal Data Protection Act" and internal corporate regulations.