**Ground Operations (Dispatch) – Information Security Management System (ISMS) – Process Review Document Part IS**

The ISMS for Ground Operations – Dispatch is aligned with regulatory obligations and the overarching security and business continuity strategies of the organization. Objectives are subject to annual review and integrated into the broader management system.

**Primary Objectives:**

1. **Protect the Confidentiality, Integrity, and Availability (CIA)** of dispatch-related data and systems.
2. **Prevent unauthorized access** to flight planning systems, aircraft movement data, and operational communication channels.
3. **Detect and respond** to information security incidents affecting dispatch functions.
4. **Ensure compliance** with applicable regulations including Regulation (EU) 2023/203.
5. **Promote competence and awareness** of information security risks within the dispatch unit.
6. **Support continuous improvement** through feedback loops and incident-driven enhancements.

**Examples:**

- Secure storage and access of OFP (Operational Flight Plan) through encrypted platforms.
- MFA on dispatch consoles and real-time monitoring of logins and data access.
- Integration of incident reporting tools aligned with IS.I.OR.215.

**Objective 1: Protect the Confidentiality, Integrity, and Availability (CIA) of dispatch-related data and systems**
**Commentary:** Protecting CIA is foundational to any ISMS. In dispatch, this applies to systems used for flight planning, real-time tracking, and coordination with ATC and internal stakeholders.
**Examples:**

- Confidentiality: Use of encrypted VPN access for remote dispatchers connecting to planning tools.
- Integrity: Implementation of checksum validation for flight plan files sent to EFBs.
- Availability: Deployment of redundant servers for the flight planning system to ensure uptime during peak traffic.

---

**Objective 2: Prevent unauthorized access to flight planning systems, aircraft movement data, and operational communication channels**
**Commentary:** Access control is critical in preventing manipulation of operationally sensitive data, particularly where dispatch supports real-time flight operations.
**Examples:**

- Role-based access control (RBAC) applied to Jeppesen and LIDO systems to restrict access by job function.
- Multi-factor authentication (MFA) for all personnel with access to dispatch consoles.
- Firewall and VPN policy enforcement to limit access from external IPs or unauthorized devices.

---

**Objective 3: Detect and respond to information security incidents impacting dispatch functions**
**Commentary:** Detection and response should be time-sensitive, especially for threats affecting live operations. Integration with a central SOC (Security Operations Centre) is beneficial.
**Examples:**

- SIEM tools (Security Information and Event Management) configured to detect anomalies in dispatch login activity and data access.
- Real-time alerting for any unauthorized data transfer or suspicious OFP – Operational Flight Plan modification.
- Incident response tabletop simulation involving a ransomware scenario targeting flight-planning databases.

---

**Objective 4: Ensure compliance with applicable regulations including Regulation (EU) 2023/203**
**Commentary:** Compliance includes establishing traceability, audit readiness, and documented procedures aligned with Part-IS and relevant AMC/GM material.
**Examples:**

- Quarterly compliance reviews using the checklist outlined in AMC1 IS.I.OR.200.
- Maintenance of a compliance matrix linking dispatch activities to EASA requirements and internal SOPs.
- Audit preparation logs showing conformity with IS.I.OR.205 and IS.I.OR.215 requirements.

**Objective 5: Promote competence and awareness of information security risks within the dispatch unit**
**Commentary:** Personnel are often the weakest link in information security. Dispatchers must understand their role in protecting data and systems.
**Examples:**

- Security awareness campaigns tailored to dispatch roles and operational scenarios.
- Annual e-learning module and knowledge test focused on dispatch-specific risks.
- Integration of cyber risk briefings into daily dispatch team meetings.

**Objective 6: Support continuous improvement through feedback loops and incident-driven enhancements**
**Commentary:** Effective ISMS must evolve. Lessons learned from incidents, internal audits, or stakeholder input should drive improvements.
**Examples:**

- Post-incident reviews that identify control failures and lead to updated dispatch SOPs.
- Regular KPI monitoring (e.g. unauthorized access attempts, system outage durations).
- Implementation of a quarterly ISMS review board where dispatch risks are presented and mitigations discussed.

## 2. Scope of the ISMS - Organisational Context

This ISMS applies specifically to the Ground Operations – Dispatch department. It covers the systems, staff, and procedures responsible for:

- Flight planning and OFP generation.
- Coordination of ATC slots and CTOTs.
- Crew briefings and real-time aircraft status updates.
- Movement control and turnaround performance.

**1. Flight Planning and Operational Flight Plan (OFP) Generation**
**Best Practices:**

- **Enforce role-based access control (RBAC) to flight planning systems such as Jeppesen or LIDO.**
- **Use encrypted channels (TLS/SSL) for all OFP distribution.**

- **Maintain version control and digital signature verification to detect unauthorized modifications.**

**Examples:**

- **A dispatcher logs into Jeppesen using multi-factor authentication (MFA) and generates an OFP with a timestamp and hash signature.**
- **Any subsequent changes to the OFP are tracked through an audit trail with alerts sent to the security dashboard.**

---

**2. Coordination of ATC Slots and Calculated Take-Off Times (CTOTs)**

**Best Practices:**

- **Integrate SIEM monitoring to detect irregularities in CTOT requests or slot changes.**
- **Synchronize slot coordination tools (e.g., Eurocontrol NOP, CHMI) with dispatch systems for real-time validation.**
- **Use whitelisting for IP ranges allowed to interact with ATC slot platforms.**

**Examples:**

- **If a CTOT update request originates from an unauthorized dispatch workstation or outside the approved VPN, an automatic block is triggered and logged.**
- **Slot coordination tools generate alerts when multiple slot changes are requested within a short window—flagging potential misuse or human error.**

---

**3. Crew Briefings and Real-Time Aircraft Status Updates**

**Best Practices:**

- **Deliver briefings through secure, authenticated platforms with digital acknowledgment (e.g., crew app or EFB portal).**
- **Mask sensitive data (e.g., passenger loads or cargo types) when not necessary for the flight crew.**
- **Link airworthiness status data securely via API integration with CAMO systems to avoid manual input errors.**

**Examples:**

- **A crew receives their pre-flight briefing through a tablet app that requires biometric login. The briefing includes current MEL items with encrypted sync from CAMO.**
- **If the EFB fails, the system logs fallback to a secure dispatch workstation with manual confirmation steps.**

---

**4. Movement Control and Turnaround Performance**

**Best Practices:**

- **Integrate real-time tracking of aircraft ground movements via ADS-B, stand allocation systems, and turnaround dashboards.**

- **Apply anomaly detection to turnaround performance data to identify possible delays or data manipulation.**
- **Restrict access to movement control data based on operational role and shift schedule.**

**Examples:**

- **Dispatchers use an integrated dashboard that combines stand availability, APU runtime, fueling, and boarding status.**
- **When an unauthorized access attempt to the turnaround metrics system is detected during non-operational hours, the account is auto-locked and reported.**

---

**5. General ISMS Integration Measures**

- **Regular Audits: Conduct quarterly audits focusing on data flow between dispatch, CAMO, ATC, and ground handling.**
- **Threat Modeling: Maintain an updated threat model that considers evolving cyber risks (e.g., ransomware targeting OFP systems).**
- **Training: Deliver job-role specific cybersecurity briefings that include simulated slot spoofing and OFP tampering scenarios.**

**Covered Assets and Interfaces**

**Digital Assets:**

- Flight planning systems (e.g. LIDO, Jeppesen).
- Slot coordination tools (e.g. NOP, CHMI).
- Crew briefing portals and EFB integration platforms.
- Dispatch communication systems (radio, VoIP).

🔍 **ISMS Risk Context: Potential Exposures for Dispatch-Covered Assets and Interfaces**

📡 **Digital Assets**

**• Flight Planning Systems (e.g. LIDO, Jeppesen)**

- *Exposure:* Unauthorized access or data breach leading to manipulation of routing, fuel calculations, or weather inputs.
  *Example:* An attacker gains access via compromised dispatcher credentials and alters alternate airport information in the OFP.

**• Slot Coordination Tools (e.g. NOP, CHMI)**

- *Exposure:* Interruption or manipulation of slot requests affecting on-time performance or causing missed CTOTs.

*Example:* Denial-of-service (DoS) attack floods the slot management interface, delaying CTOT confirmation messages.

- **Crew Briefing Portals and EFB Integration Platforms**
  - *Exposure:* Malicious modification or interception of crew briefing packets during transfer to the Electronic Flight Bag (EFB).
    *Example:* An outdated EFB synchronizes over unsecured Wi-Fi, allowing a man-in-the-middle (MITM) attack to modify briefing content.
- **Dispatch Communication Systems (Radio, VoIP)**
  - *Exposure:* Eavesdropping or spoofing of critical voice communications, particularly during time-sensitive turnaround decisions.
    *Example:* A VoIP system is compromised, allowing an intruder to issue false instructions posing as operations.

**Physical Assets:**

- Dispatch consoles and workstations.
- Backup communication and power systems.
- Hard copy NOTAMs and OFP archives.

- **Dispatch Consoles and Workstations**
  - ***Exposure:* Physical access to unattended or unlocked consoles allows unauthorized manipulation of flight data.**
    ***Example:* A ground service employee accesses an open dispatch console and extracts confidential route planning files to a USB drive.**
- **Backup Communication and Power Systems**
  - ***Exposure:* Backup systems are poorly maintained or untested, leading to total communication failure during a primary system outage.**
    ***Example:* A UPS (uninterruptible power supply) fails during a power outage, resulting in the loss of radio dispatch functionality for outbound flights.**
- **Hard Copy NOTAMs and OFP Archives**
  - ***Exposure:* Sensitive paper documents left unsecured or improperly destroyed, increasing the risk of data leaks.**
    ***Example:* An OFP archive bin near the dispatch desk is accessed by cleaning staff and confidential documents are removed and photographed.**

**Interfaces:**

- **Flight Operations** – via flight crew briefings, MEL/CDL communication.
- **Maintenance (CAMO/AMO)** – to assess dispatch impact of technical defects.
- **Security** – access to secure areas and contingency scenarios.
- **Airport Authorities/ATC** – data sharing for real-time coordination.

**Flight Operations (via flight crew briefings, MEL/CDL communication)**

- *Exposure:* Dispatch provides briefing based on outdated or incomplete Minimum Equipment List (MEL) data due to miscommunication.
  *Example:* An incorrect MEL entry results in an OFP that does not reflect fuel penalties, potentially violating dispatch requirements.

**• Maintenance (CAMO/AMO)**

- *Exposure:* Delay in technical status updates or unauthorized access to aircraft technical records shared digitally.
  *Example:* A vulnerability in the interface between the CAMO system and dispatch planning tools allows exposure of defect reports before rectification.

**• Security (Access to secure areas, contingency scenarios)**

- *Exposure:* Security system misconfigurations allow unauthorized personnel to enter dispatch zones during shift changes.
  *Example:* A terminated employee retains an active badge and enters the dispatch center after hours, compromising systems and data.

**• Airport Authorities/ATC (Real-time coordination)**

- *Exposure:* Data integrity issues or transmission errors disrupt coordination with ground authorities or ATC.
  *Example:* Real-time turnaround data shared with ATC is delayed or misaligned due to a misconfigured API, resulting in a mis-sequenced departure.

### 3. Roles & Responsibilities

- **Dispatch Manager:** Accountable for ISMS implementation in Ground Ops – Dispatch.
- **Flight Dispatchers:** Execute operational planning securely and report anomalies.
- **IT Support (Ops Systems):** Ensure uptime, backups, and access management for dispatch tools.

- **Security Liaison Officer:** Coordinates threat and incident handling with the Security Department.
- **Compliance Officer:** Ensures regulatory alignment, audit readiness, and ISMS conformance.

**4. Stakeholders & Interfaces**

**Internal Stakeholders:**

- **Flight Operations:** Alignment on aircraft release, MEL limitations, and PIREPs.
- **CAMO:** Integration of maintenance status and dispatch feasibility.
- **Ground Handling:** Turnaround status reports and event escalation.
- **Security:** Access control for dispatch areas, threat escalation protocols.

**. Digital Assets – Potential Exposures**
**a) Flight Planning Systems (e.g. LIDO, Jeppesen)**
**Exposure: Unauthorized access, data tampering, and unavailability of the system. Example: A dispatcher's login credentials are phished, allowing an attacker to alter fuel calculation parameters and alternate airport selections in the OFP, potentially leading to operational disruption or safety risk.**

**b) Slot Coordination Tools (e.g. NOP, CHMI)**
**Exposure: CTOT manipulation, denial-of-service (DoS), or data corruption. Example: Attackers flood the CHMI web service with requests, temporarily disabling access and delaying slot requests for time-sensitive departures.**

**c) Crew Briefing Portals and EFB Integration Platforms**
**Exposure: Loss of confidentiality and data integrity during synchronization. Example: A pilot's EFB connects to a public Wi-Fi network and syncs with the briefing portal. A man-in-the-middle (MITM) attacker intercepts and modifies critical NOTAM information.**

**d) Dispatch Communication Systems (Radio, VoIP)**
**Exposure: Eavesdropping, spoofing, or unavailability during critical phases. Example: VoIP communications are routed through an unsecured network switch. A malicious actor gains access and listens in on real-time dispatch decisions involving load distribution.**

---

**2. Physical Assets – Potential Exposures**

**a) Dispatch Consoles and Workstations**

**Exposure: Unauthorized physical access or tampering with terminals. Example: A shift handover is poorly executed and an unattended, unlocked console remains accessible. A third party extracts flight schedules and OFP archives using a USB device.**

**b) Backup Communication and Power Systems**
**Exposure: System failure due to poor maintenance or lack of redundancy. Example: During a power outage, the backup power source fails to activate due to battery degradation, resulting in a total communication blackout affecting four scheduled flights.**

**c) Hard Copy NOTAMs and OFP Archives**
**Exposure: Information leakage, improper disposal, or loss. Example: a visitor passing through the restricted zone photographs printed OFPs left unattended on a desk during break time.**

---

**3. Interfaces – Potential Exposures**
**a) Flight Operations (Briefings, MEL/CDL Communication)**
**Exposure: Misinformation or failure to receive updated MEL/CDL data. Example: The MEL update on a failed pitot tube is delayed. The OFP issued without this information causes the crew to rely on incorrect performance data.**
**b) Maintenance (CAMO/AMO)**
**Exposure: Delay or compromise of technical status updates. Example: CAMO-to-dispatch interface software has a configuration error that prevents defect reports from reaching dispatch, resulting in the aircraft being released without full operational awareness.**
**c) Security (Access Control, Contingency Coordination)**
**Exposure: Unauthorized facility access or inadequate coordination during incidents. Example: A security badge system error allows a former employee to enter the dispatch control area, gaining access to flight tracking dashboards and OFP generation tools.**
**d) Airport Authorities/ATC (Real-Time Coordination)**
**Exposure: Data mismatch, latency, or unauthorized transmission. Example: A misconfigured XML feed sends inaccurate turnaround completion times to ATC, resulting in out-of-sequence take-off slot planning and an avoidable departure delay.**

**External Stakeholders:**

- **Air Traffic Control (ATC) and Slot Coordinators:** Data exchange and contingency rerouting.
- **Airport Authorities:** Real-time ground status and emergency coordination.
- **Third-party Providers:** Cloud-based dispatch system vendors, network infrastructure partners.

Engagement with external stakeholders introduces complex and layered security dependencies. The Dispatch ISMS must include:

- Formal data exchange agreements and SLAs with ATC, airport, and vendor systems.
- Regular third-party risk assessments and secure onboarding procedures.
- Real-time monitoring, endpoint hardening, and interface-level encryption.
- Incident response protocols that extend to partner systems, including predefined contingency workflows.

These safeguards ensure the Dispatch unit maintains operational continuity, data integrity, and regulatory compliance across all stakeholder interfaces.

**1. Air Traffic Control (ATC) and Slot Coordinators**
**Functional Scope:** Data exchange for flight planning, CTOT management, and real-time contingency rerouting.
**Exposures:**

- **Data Integrity Compromise:** If malicious actors intercept or alter CTOT messages or slot confirmation exchanges, the aircraft may be dispatched with outdated or invalid permissions.
- **Service Unavailability:** Overload or denial-of-service attacks on slot coordination platforms could prevent timely submissions, leading to delays or forced cancellations.
- **Authentication Weaknesses:** Lack of secure channel authentication can expose slot allocation data to spoofing.

**Example:** An attacker simulates legitimate ATC communication and sends a false slot reassignment, resulting in a misaligned departure window and operational disruption.

---

**2. Airport Authorities**
**Functional Scope:** Coordination of aircraft stand allocation, emergency response, turnaround tracking, and general airside operations.
**Exposures:**

- **Data Latency or Loss:** Delays in receiving or transmitting critical turnaround data (e.g., fueling status or stand availability) may affect dispatch-planning accuracy.
- **Access Control Breaches:** Inadequate segregation between airport-operated and airline systems could allow unauthorized access to sensitive dispatch data.

- **Contingency Coordination Gaps:** During emergencies, unclear or unsecured communication channels may hinder effective response.

**Example:** Due to improper firewall configuration, an external airport contractor gains unintended access to dispatch system telemetry, exposing sensitive data related to fleet readiness.

---

**3. Third-party Providers**
**Functional Scope:** Provision of cloud-hosted dispatch software, flight-planning systems, infrastructure support (e.g., VPN, backup comms).
**Exposures:**

- **Supply Chain Vulnerabilities:** Third-party systems may serve as attack vectors if they are not aligned with equivalent security baselines.
- **Uncontrolled Data Sharing:** Poorly governed APIs between dispatch systems and third-party platforms may result in unintended data exposure.
- **Reliance on External Availability:** If a third-party cloud platform experiences outages, dispatch operations may be unable to access critical planning tools.

**Example:** A misconfigured API used by a cloud-based OFP system unintentionally exposes routing data of all scheduled flights to an external web crawler, creating a significant confidentiality breach.

## 5. Compliance & Standards Alignment

The ISMS for Dispatch is compliant with:

- **Regulation (EU) 2023/203** and AMC/GM from ED Decisions 2023/008–010.
- **IS.I.OR.200–260**: Covering the full lifecycle of ISMS implementation.
- **NIST CSF and ISO/IEC 27001**: As referenced in AMC1 IS.I.OR.200 (e).

## 6. Incident Detection, Response & Recovery

Aligned with **IS.I.OR.220**, the Dispatch ISMS includes:

- Defined severity levels for disruptions (e.g. outage of slot coordination vs. full OFP server failure).
- Escalation workflows for service interruption affecting scheduled departures.
- Contingency plans for fallback to manual OFP generation and radio-based communication.

- Post-incident reviews logged and shared with the ISMS Steering Committee.

**7. Training & Awareness**

Security training for Dispatch includes:

- Role-based cybersecurity awareness.
- Phishing simulation exercises.
- Emergency handling procedures.
- Daily pre-shift briefings on data handling protocols.

**8. Continuous Improvement**

The Dispatch ISMS includes:

- Regular KPI reviews (e.g. average response time to OFP data errors).
- Audit findings remediation tracking.
- Tabletop exercises simulating cyber interference in dispatch systems.
- Annual ISMS policy review aligned with organizational risk strategy.

**Developing a Risk Register to reflect the Risks found in the Dispatch business Area**

**Digital Asset Risks**

1. **Unauthorized Access to Flight Planning Systems** – Credential compromise (e.g., phishing) leading to altered flight plans or rerouting.
2. **OFP Tampering or Corruption** – Injection of manipulated data into the Operational Flight Plan affecting routing, fuel, or alternate airport information.
3. **CTOT Data Manipulation** – Alteration or spoofing of ATC slot allocation, resulting in timing disruptions.
4. **Denial of Service (DoS) on Slot Coordination Tools** – Flooding platforms like NOP or CHMI, preventing timely CTOT submissions.
5. **EFB Sync Interception (MITM Attack)** – Crew briefings or NOTAMs altered during sync over unsecured networks.

6. **VoIP Communication Spoofing** – False instructions issued during real-time ground handling via compromised voice systems.
7. **SIEM Bypass or Blind Spots** – Failure to detect anomalies due to poorly configured monitoring systems.
8. **Insecure API Exposure** – Improperly governed API integrations exposing sensitive data to unauthorized third parties.

**Physical Asset Risks**

9. **Unattended Dispatch Consoles** – Physical access by unauthorized persons resulting in data theft or manipulation.
10. **Hard Copy OFP/NOTAM Theft or Exposure** – Sensitive documents left unsecured or improperly disposed.
11. **Backup System Failure** – Communication blackout during outages due to untested or degraded UPS systems.
12. **Unauthorized USB/Device Access** – Data exfiltration via unmonitored ports or removable media.

**Operational Process Risks**

13. **MEL/CDL Data Outdated or Inaccurate** – OFP issued with incorrect dispatch constraints due to lag in MEL/CDL updates.
14. **CAMO–Dispatch Integration Error** – Aircraft released without up-to-date defect or airworthiness information due to sync failure.
15. **Crew Briefing Delivery Failure** – Failure of secure delivery mechanisms affecting situational awareness.
16. **Incorrect Turnaround Metrics** – Compromised or manipulated data leading to misinformed dispatch decisions.
17. **Anomaly Detection Failures in Turnaround Systems** – Late identification of delays, increasing AOG risk.

**Interface & Communication Risks**

18. **Real-Time Data Mismatch with ATC** – Inaccurate data causing sequencing or slot planning issues.

19. **Airport Systems Access Breach** – Airport-side access control errors allowing unauthorized entry into dispatch systems.
20. **Compromised CAMO Interface** – Misuse of CAMO access resulting in exposure of technical records.
21. **Security Access Mismanagement** – Inactive or invalid badges remaining active and exploited post-termination.
22. **Contingency Coordination Breakdown** – Inability to coordinate due to lack of secure communication during emergencies.

**External Stakeholder Risks**

23. **ATC Slot Spoofing** – False slot confirmation via unverified communications leading to misaligned aircraft sequencing.
24. **Cloud Provider Outage** – Unavailability of third party OFP tools due to cloud downtime, disrupting dispatch operations.
25. **Supply Chain Cyber Weakness** – Third-party software or VPN platforms becoming vectors for malware or unauthorized access.
26. **Third-Party API Misconfiguration** – Data leaks via public exposure or flawed integration.
27. **SLAs Not Enforced** – Service delivery or availability issues not captured in supplier agreements (e.g., CTOT platform resilience).

**Human & Training Risks**

28. **Social Engineering Attacks on Dispatchers** – Manipulative techniques used to extract credentials or authorize bad actors.
29. **Training Deficiencies in Incident Handling** – Inadequate preparedness for ransomware or data breach recovery.
30. **Neglected Awareness Campaigns** – Dispatchers unaware of phishing, spoofing, or access risks.
31. **Role Confusion During Incidents** – Delay or failure in response due to unclear escalation paths.

**Compliance & Process Control Risks**

32. **Lack of Traceability for OFP Changes** – Poor version control or audit trails undermining accountability.
33. **Non-Conformity with Regulation (EU) 2023/203** – Incomplete implementation of AMC1 IS.I.OR.200 (e) leading to compliance gaps.
34. **ISMS Review Delays** – Missed updates to ISMS policies, increasing exposure to evolving threats.

**Risk Treatment -** These risks should be cataloged in your centralized risk register with full details per the format:

- **Risk Description**
- **Source / Threat Vector**
- **Impact (CIA)**
- **Risk Owner**
- **Risk Category (Digital, Physical, Interface, etc.)**
- **Treatment Plan**
- **Status and Review Date**