SOP-10 — Incident Response

Triggers (non-exhaustive):

- Operator cancellation, AOG, or aircraft swap on a confirmed flight.
- Sanctions match (true or unresolved).
- Cash payment that may require Form 8300.
- Suspected fraud, payment chargeback or insolvency of a counterparty.
- Personal data breach.
- Regulatory inquiry (DOT, FAA, IRS, OFAC, FinCEN, EU DPA, CAA, ENAC, LBA, DGAC, FINMA, …).
- Media inquiry related to a passenger / aircraft incident.

Common playbook

1. **Stabilise the customer first.** If a flight is affected, the priority is to keep the passengers safe, informed and re-accommodated.
2. **Open an incident ticket** in the Compliance log: who, what, when, where, evidence trail.
3. **Notify Compliance Officer within 1 hour** of detection, regardless of business hours.
4. **Preserve evidence** — do not delete emails, messages or files; export the booking file.
5. **Containment** — for IT/data: rotate credentials, isolate affected systems. For sanctions: quarantine funds. For regulator inquiry: confirm receipt, do not respond substantively before counsel review.
6. **Notification clocks:**
7. Personal data breach: 72 hours to lead SA (Art. 33 GDPR) where triggered.
8. Form 8300: 15 days.
9. OFAC voluntary self-disclosure: as soon as practicable.
10. Insurance: per the policy notice clause (often "as soon as practicable" and never later than 30 days).
11. **Customer communication** — Compliance approves any external statement.
12. **Lessons learned** — within 30 days of closure, a written post-mortem identifying root cause and corrective actions; the SOPs and policies above are updated as needed.