



INFORMATION SECURITY POLICY

Alidaunia Training Srl riconosce il ruolo critico dell'Information Security nel mantenimento della Safety e si impegna a garantire la riservatezza, l'integrità, l'autenticità e la disponibilità degli asset informativi attraverso l'istituzione e il mantenimento di un Information Security Management System (ISMS), in conformità ai requisiti della EASA Part-IS e agli ulteriori obblighi legali, regolamentari e contrattuali applicabili.

- **Conformità normativa e agli standard:** ci impegniamo a rispettare tutta la normativa nazionale ed europea applicabile e gli obblighi contrattuali in materia di Information Security. Saranno inoltre considerati gli standard internazionali e le best practices di riferimento (es. ISO/IEC 27001, linee guida EASA), al fine di garantire un approccio proattivo nella gestione dei rischi di Information Security.
- **Obiettivi e indicatori di performance:** saranno definiti obiettivi chiari e misurabili, nonché indicatori di performance, per monitorare e migliorare il livello di Information Security. Tali obiettivi saranno periodicamente riesaminati dal senior management e integrati negli obiettivi generali di Safety e operatività aziendale.
- **Principi, attività e processi di sicurezza:** saranno definiti e mantenuti adeguati principi, processi e attività per la protezione dei sistemi informativi e dei dati aziendali, inclusi, a titolo esemplificativo ma non esaustivo, valutazione dei rischi, controllo degli accessi, cifratura dei dati, gestione degli incidenti e pratiche di sviluppo sicuro del software.
- **Integrazione dei requisiti ISMS:** l'organizzazione si impegna a integrare i principi e i requisiti dell'information Security Management System in tutti i processi aziendali, assicurando che l'Information Security sia parte integrante delle attività operative e dei processi decisionali a ogni livello organizzativo.
- **Miglioramento continuo e maturità del sistema:** l'organizzazione perseguirà il miglioramento continuo del proprio livello di maturità in materia di Information Security, assicurando che politiche, pratiche e controlli evolvano in risposta alle nuove minacce e agli sviluppi tecnologici.
- **Allocazione delle risorse:** saranno garantite risorse adeguate, in termini umani, finanziari e tecnologici, per l'implementazione, il mantenimento e il miglioramento continuo del Information Security Management System e delle attività correlate.
- **Responsabilità manageriale:** l'Information Security rappresenta una responsabilità condivisa all'interno dell'organizzazione. A tutti i responsabili aziendali è attribuita la responsabilità di garantire che i rischi relativi all'information Security siano identificati, gestiti e segnalati nell'ambito delle rispettive aree di competenza.
- **Formazione e consapevolezza:** saranno svolte periodicamente attività di formazione e sensibilizzazione per garantire che tutto il personale comprenda la presente policy, le proprie responsabilità e le procedure applicabili. Tali attività saranno aggiornate e ripetute in caso di modifiche significative.
- **Just Culture e segnalazione degli eventi:** l'organizzazione promuove una "Just Culture" che incoraggia il personale a segnalare vulnerabilità, eventi sospetti o anomali e incidenti relativi all'Information Security senza timore di colpa o ritorsioni, favorendo trasparenza e tempestiva mitigazione dei rischi.
- **Comunicazione con le parti interessate:** la presente policy sarà comunicata a tutte le parti interessate rilevanti, interne ed esterne, inclusi partner e fornitori di servizi, al fine di garantire una comprensione condivisa e un'applicazione coerente degli obiettivi di Information Security.

Foggia, 06/02/2026

Approvato da
Alidaunia Training S.r.l.
Accountable Manager

