

Scopo

Lo scopo della presente politica è quello di indicare linee di indirizzo per definire, pianificare, attuare e mantenere aggiornato un sistema di gestione della sicurezza delle informazioni allo scopo di proteggere gli asset informativi dell'organizzazione da tutte le minacce, interne o esterne, dolose o accidentali.

L'azienda si impegna a garantire che:

- Tutte le Informazioni siano protette contro accessi non autorizzati;
- Siano garantite la Riservatezza, l'Integrità e la Disponibilità delle informazioni;
- Siano soddisfatti i requisiti normativi, legislativi, contrattuali, regolamentari e qualsiasi altro requisito sottoscritto dall'azienda;
- Vengano realizzati, mantenuti e testati ad intervalli regolari i Business Continuity Plan;
- Sia perseguito il miglioramento continuo dei processi del sistema e dell'efficacia delle azioni di trattamento del rischio secondo un approccio PDCA;
- La formazione sulla sicurezza delle informazioni (on boarding e successivi aggiornamenti) sia obbligatoria per tutto il personale;
- Tutte le violazioni della sicurezza delle informazioni, reali o potenziali, vengano segnalate e indagate dal Team Sicurezza Informazioni
- Il sistema di gestione della sicurezza delle informazioni (ISMS) sia conforme agli standard ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2020, garantendo l'applicazione di tutte le misure di controllo ivi previste

Obiettivi

Gli obiettivi di questa Policy sulla sicurezza delle informazioni sono di garantire:

- La Business Continuity, tramite il contenimento delle interruzioni o danni al Business limitando l'impatto degli incidenti di sicurezza delle informazioni;
- La riduzione dei rischi legati alla Riservatezza, Integrità e Disponibilità delle informazioni a un livello accettabile;
- Il raggiungimento ed il mantenimento della conformità del sistema di gestione della sicurezza delle informazioni agli standard ISO/IEC 27001:2022, ISO/IEC 27017:2021 e ISO/IEC 27018:2020.

Responsabilità

La Responsabilità primaria a livello global in merito alla gestione della sicurezza delle informazioni è in capo al CISO (Chief Information Security Officer), all'ISF (Information Security Forum) ed al ISM (Information Security Manager).

La Responsabilità a livello local di garantire la diffusione della presente politica e l'efficace applicazione del sistema di gestione della sicurezza delle informazione spetta al General Manager South Europe ed Plant Manager Italy con il supporto del Coordinatore Locale per la Protezione dei Dati (LDPC).

Tutti i line manager sono responsabili della corretta applicazione di questa politica all'interno dei loro reparti.

Tutti i dipendenti, ciascuno nell'ambito delle rispettive attribuzioni e competenze, sono responsabili di seguire le policy, le procedure e le istruzioni del sistema di gestione della sicurezza delle informazioni (ISMS) e di segnalare qualsiasi violazione di cui vengano a conoscenza.

Ortona 09/04/2025

LDPC Italy

General Manager South Europe

Plant Manager Italy

ORT-POL-031 V02

