POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

L'*Alta Direzione* di P.E. LABELLERS SPA riconosce la sicurezza delle informazioni un elemento strategico fondamentale per la continuità del business, la competitività sul mercato e la fiducia dei propri clienti, partner e stakeholder. Le informazioni trattate, siano esse tecniche, produttive, commerciali o personali, costituiscono un patrimonio aziendale di primaria importanza che deve essere protetto da minacce interne ed esterne.

Con l'intento di proteggere le informazioni aziendali garantendone riservatezza, integrità e disponibilità, PE LABELLERS S.P.A. si è dotata di un Sistema di Gestione della Sicurezza delle Informazioni improntato sulla norma ISO/IEC 27001:2022.

Ciò comporta l'impegno aziendale nella progettazione, implementazione e continuo miglioramento di un Sistema di Gestione della Sicurezza delle Informazioni che tiene in considerazione e soddisfi un insieme eterogeneo di requisiti, costituito dai Requisiti delle norme della serie ISO/IEC 27000 nonché del Regolamento (UE) 2016/679 – GDPR.

La presente Politica si applica a tutte le informazioni trattate da P.E. LABELLERS nei propri processi, sistemi e servizi, incluse:

- informazioni dei clienti e dei partner commerciali,
- dati relativi a processi produttivi e progetti di innovazione,
- dati personali trattati nell'ambito delle attività aziendali,
- documentazione tecnica, finanziaria e gestionale,
- know-how e proprietà intellettuale.

La politica copre tutte le sedi operative, tutti i reparti e le funzioni aziendali, nonché i fornitori e i partner che accedono alle informazioni aziendali.

L'*Alta Direzione* si impegna a:

- **Proteggere** riservatezza, integrità e disponibilità delle **informazioni trattate**,
- **Implementare e mantenere un SGSI** conforme alla ISO/IEC 27001:2022,
- Fissare **obiettivi** di sicurezza delle informazioni misurabili e allinearli alla strategia aziendale,
- Rispettare i **requisiti normativi e contrattuali** applicabili, inclusi il GDPR e le normative nazionali/internazionali,
- **classificare le informazioni** trattate all'interno dell'organizzazione, in modo da garantire un'adeguata protezione in funzione della loro criticità, riservatezza e valore per l'azienda e per le parti interessate,
- garantire la **gestione dei rischi** basata su un'analisi sistematica e periodica.
- **Sensibilizzare e formare il personale** sul proprio ruolo in materia di sicurezza delle informazioni,
- Garantire **risorse adeguate** all'attuazione, al mantenimento e al miglioramento del SGSI,
- Garantire il **miglioramento continuo** del SGSI attraverso le revisioni periodiche della politica e del sistema di gestione, il monitoraggio delle performance di sicurezza, le azioni correttive e

preventive basate su audit e incidenti, e l'aggiornamento continuo in base a nuove minacce, tecnologie e normative.

OBIETTIVI DI SICUREZZA

Gli obiettivi principali di P.E. LABELLERS SPA in materia di sicurezza delle informazioni sono:

1. Assicurare la riservatezza dei dati dei clienti, dei partner e dell'azienda stessa,
2. Preservare l'integrità delle informazioni durante tutte le fasi di gestione,
3. Garantire la disponibilità delle informazioni e dei sistemi critici, assicurando la continuità operativa,
4. Ridurre il numero di incidenti di sicurezza e accessi non autorizzati,
5. Mantenere aggiornate le misure di sicurezza fisica e logica,
6. Prevenire e gestire tempestivamente eventuali incidenti di sicurezza,
7. Promuovere una cultura diffusa della sicurezza delle informazioni,
8. Monitorare le prestazioni del SGSI attraverso audit, KPI e riesami periodici.

CONTROLLI DI SICUREZZA

P.E. LABELLERS SPA applica controlli di sicurezza coerenti con i requisiti della norma e basati sulla valutazione del rischio, che includono:

- Gestione dei rischi: analisi e mitigazione dei rischi informativi,
- Gestione degli accessi: autorizzazioni basate sul minimo privilegio e autenticazione sicura,
- Protezione dei dati: crittografia, backup e protezione fisica/logica degli asset,
- Continuità operativa: piani e test di continuità aziendale e disaster recovery,
- Gestione degli incidenti: procedure di rilevamento, analisi e risposta agli eventi di sicurezza,
- Conformità normativa: rispetto di GDPR e leggi applicabili,
- Governance: definizione di ruoli, responsabilità e riesame periodico della politica.

La presente Politica è stata approvata dall'*Alta Direzione* e viene resa disponibile alle parti interessate tramite la pubblicazione sul sito aziendale e la comunicazione a tutti i dipendenti, collaboratori e fornitori.

Data: 03/02/2026

La Direzione: