POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

COELME S.p.A. riconosce che le informazioni e i dati costituiscono un patrimonio di fondamentale valore strategico per le proprie attività, la continuità del business e la fiducia di clienti, fornitori e partner. Per questo motivo, la Società ha scelto di adottare e perfezionare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) in piena conformità alla norma UNI CEI EN ISO/IEC 27001:2024.

La Direzione formalizza il proprio impegno prioritario nell'assicurare la protezione delle informazioni trattate, garantendo la disponibilità tempestiva e costante delle risorse umane, tecnologiche ed economico-finanziarie necessarie per il raggiungimento degli obiettivi aziendali e per il miglioramento continuo del Sistema di Gestione.

La gestione della sicurezza delle informazioni all'interno di COELME S.p.A. si fonda sui quattro pilastri cardine del modello di protezione dati:

- Riservatezza (Confidentiality): Garantire che le informazioni, i dati sensibili e riservati siano accessibili ed esaminabili esclusivamente dai soggetti (utenti, processi o sistemi) debitamente autorizzati, prevenendo qualsiasi forma di divulgazione o accesso non autorizzato.
- Integrità (Integrity): Salvaguardare la precisione, l'accuratezza, la completezza e l'inalterabilità delle informazioni e dei metodi di elaborazione durante tutte le fasi del loro ciclo di vita (creazione, trasmissione, elaborazione, archiviazione).
- Disponibilità (Availability): Assicurare che le informazioni, i sistemi informativi, le reti e le applicazioni aziendali siano tempestivamente fruibili e accessibili agli utenti autorizzati ogni volta che ne abbiano necessità nell'ambito delle attività operative.
- Autenticità (Authenticity): Garantire che le informazioni, i dati, i servizi o le identità dei soggetti (utenti, processi o dispositivi) siano autentici, verificabili e non contraffatti, e che provengano effettivamente dalla fonte dichiarata.

COELME S.p.A. integra nei propri processi aziendali principi avanzati di resilienza e continuità aziendale per salvaguardare l'organizzazione da eventi avversi imprevisti, emergenze o attacchi cibernetici:

- Resilienza Informatica e Organizzativa: Progettare e mantenere sistemi, reti e infrastrutture capaci di prevenire, resistere, assorbire e reagire tempestivamente a guasti tecnici, errori umani, disastri naturali o attacchi informatici (cyber-attacchi), garantendo la continuità dei servizi essenziali
- Business Continuity & Disaster Recovery: Definire, documentare e testare periodicamente le procedure di Business Continuity e i Piani di Ripristino del Disastro (DRP) per garantire il rapido ripristino dei processi critici.

COELME S.p.A. adotta le seguenti linee guida e indirizzi strategici:

- Valutazione e Gestione dei Rischi: Identificare e valutare sistematicamente i rischi relativi alla gestione delle informazioni e delle infrastrutture tecnologiche, analizzando minacce rispetto ai requisiti di riservatezza, integrità, disponibilità, autenticità e resilienza.

- Conformità Normativa e Legale: Garantire la rigorosa applicazione delle leggi e dei regolamenti vigenti (es. GDPR - Regolamento UE 2016/679, normative sulla cybersicurezza e direttive nazionali/europee) e di ogni altro requisito sottoscritto dall'organizzazione.
- Misure di Protezione e Controlli: Attuare contromisure logiche, fisiche e organizzative idonee a proteggere i dati da accessi o modifiche non autorizzate.
- Prevenzione e Gestione degli Incidenti: Implementare procedure di monitoraggio continuo e gestione tempestiva delle anomalie della sicurezza, assicurando l'analisi approfondita delle cause e l'adozione di azioni correttive mirate.
- Formazione e Consapevolezza del Personale: Promuovere la formazione continua ed il periodico addestramento del personale, dei collaboratori e dei fornitori chiave rispetto alle minacce cyber correnti (phishing, social engineering) e alle corrette prassi operative.
- Miglioramento Continuo e Coinvolgimento: Consolidare i rapporti di collaborazione con tutte le parti interessate (clienti, fornitori, autorità) per il continuo efficientamento del Sistema di Gestione della Sicurezza delle Informazioni.

L'applicazione del Sistema di Gestione richiede la piena partecipazione, l'impegno costante e la consapevolezza di tutto il personale dipendente e di tutti coloro che operano per conto dell'Azienda.

Gli obiettivi operativi specifici e le azioni di sicurezza vengono definiti annualmente in sede di Riesame della Direzione. La presente Politica viene riesaminata almeno una volta all'anno in occasione del Riesame della Direzione e/o ogniqualvolta intervengano cambiamenti significativi (organizzativi, tecnologici, normativi o di contesto), al fine di accertarne la continua idoneità, adeguatezza ed efficacia.

Il presente documento è pubblico, comunicato a tutti i collaboratori interni ed esterni e reso liberamente disponibile per la consultazione da parte di tutte le parti interessate.

Santa Maria di Sala (VE), 22.10.2026

La Direzione