La presente **Policy Generale di Sicurezza delle Informazioni** (Ver. 1.0) esprime l'impegno della Direzione di **RIPET S.r.l.** nel proteggere la riservatezza, l'integrità e la disponibilità delle informazioni proprie e di quelle affidate da clienti, consorzi e parti terze. Essa costituisce il documento di vertice del Sistema di Gestione per la Sicurezza delle Informazioni (di seguito ISMS) e stabilisce gli obiettivi, i principi e le responsabilità a cui tutte le policy, le procedure e i controlli di dettaglio devono conformarsi.

La presente policy si fonda su **ISO/IEC 27001:2022** e relativo Amendment 1:2024, sulle linee guida ISO/IEC 27002:2022, sul Regolamento (UE) 2016/679 (GDPR) e sul D.Lgs. 196/2003 e s.m.i. Si integra inoltre con il Sistema di Gestione Ambientale ISO 14001 già certificato e con il Modello di Organizzazione, Gestione e Controllo ex D.Lgs. 231/2001 adottati dall'organizzazione, riutilizzandone, ove possibile, procedure e strumenti. Costituisce il riferimento sovraordinato per tutte le policy e procedure dell'ISMS.

L'ISMS di RIPET copre la progettazione, produzione, vendita e assistenza di eco-compattatori (reverse vending machine) per la raccolta selettiva di PET, vetro e alluminio, nonché l'erogazione dei servizi IoT di monitoraggio remoto delle macchine installate tramite la piattaforma propria.

La policy si applica a tutto il personale dipendente, ai membri della Direzione e del Consiglio di Amministrazione, ai collaboratori, ai manutentori esterni che operano sul campo e a qualsiasi fornitore o consulente che acceda alle informazioni, ai sistemi o alle sedi di RIPET. Rientrano nel perimetro i sistemi informativi d'ufficio, i sistemi informativi aziendali e i servizi cloud utilizzati, l'infrastruttura delle macchine IoT installate presso i clienti, la piattaforma propria e i relativi servizi di hosting, indipendentemente dal fatto che siano gestiti internamente o da fornitori esterni.

Ai fini del presente documento si intende per informazione qualsiasi dato o conoscenza di valore per l'organizzazione, in formato elettronico o cartaceo. La sicurezza delle informazioni è la preservazione di riservatezza, integrità e disponibilità (la cosiddetta triade CIA): la *riservatezza* garantisce che le informazioni siano accessibili solo a chi è autorizzato, l'*integrità* ne tutela accuratezza e completezza, la *disponibilità* assicura che siano fruibili quando servono. Per ISMS si intende l'insieme coordinato di politiche, procedure, ruoli e controlli con cui RIPET gestisce la sicurezza delle informazioni. Un rischio è la combinazione della probabilità che una minaccia sfrutti una vulnerabilità e dell'impatto conseguente; un incidente di sicurezza è un evento, singolo o in serie, che compromette o può compromettere la triade CIA.

RIPET adotta un approccio alla sicurezza delle informazioni basato sul rischio e proporzionato alla propria dimensione, alla natura del business e al valore degli asset trattati. La protezione delle informazioni non è un obiettivo tecnico fine a sé stesso, ma una condizione per garantire la continuità del servizio IoT erogato h24, tutelare il patrimonio di proprietà intellettuale dell'azienda e onorare gli impegni di cybersecurity assunti verso i clienti e il Consorzio di riferimento.

Coerentemente con le priorità definite dalla Direzione, l'ordine di rilevanza degli obiettivi di sicurezza è il seguente: la **disponibilità** dei sistemi, in ragione del servizio continuativo di monitoraggio delle macchine; la **riservatezza** dei dati, con riferimento ai brevetti, alla proprietà intellettuale e ai dati dei clienti; e l'**integrità** delle informazioni di raccolta e telemetria. Tale ordine orienta le scelte di trattamento del rischio quando si rendono necessari compromessi.

L'ISMS si ispira ai principi del minimo privilegio e del need-to-know, per cui ogni soggetto accede esclusivamente alle informazioni e alle funzioni necessarie al proprio ruolo; alla difesa in profondità, che combina misure tecniche, fisiche e organizzative; e alla segregazione dei compiti dove la dimensione organizzativa lo consente. La sicurezza è considerata sin dalla progettazione di nuovi sistemi e servizi (security by design) e il miglioramento continuo è perseguito attraverso il ciclo Plan-Do-Check-Act, in coerenza con la prassi già consolidata dai sistemi di gestione ISO 14001 e 231.

La Direzione di RIPET, nella persona dell'Amministratore Delegato Alessandro Persia, assume la responsabilità complessiva dell'ISMS e ne garantisce l'integrazione nei processi aziendali. La Direzione approva la presente policy e gli obiettivi di sicurezza, assicura la disponibilità delle risorse necessarie all'implementazione e al mantenimento del sistema, promuove la consapevolezza del personale e verifica periodicamente, in sede di riesame della direzione, l'adeguatezza e l'efficacia dei controlli adottati. La Direzione si impegna inoltre al rispetto dei requisiti applicabili, legali, contrattuali e regolamentari, e al miglioramento continuo dell'ISMS.

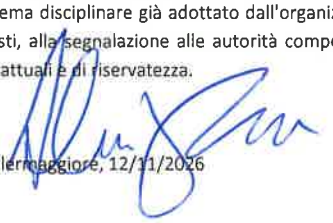
La sicurezza delle informazioni in RIPET è governata da un processo strutturato di valutazione e trattamento del rischio. I rischi sono riesaminati almeno annualmente e in occasione di cambiamenti significativi del contesto, dell'infrastruttura o delle minacce.

La Direzione definisce gli indirizzi strategici, approva le policy e gli obiettivi e assegna le risorse. RIPET si avvale anche di fornitori qualificati, ai quali richiede livelli di sicurezza adeguati, secondo un modello di responsabilità condivisa. I fornitori che erogano servizi rilevanti per la sicurezza sono responsabili della sicurezza nell'ambito delle rispettive forniture, secondo un modello di responsabilità condivisa.

Tutto il personale e i collaboratori hanno il dovere di conoscere e rispettare le policy applicabili, di proteggere le informazioni e gli asset affidati e di segnalare tempestivamente eventi e incidenti di sicurezza secondo quanto previsto dalla Policy di Gestione degli Incidenti.

L'efficacia dell'ISMS è verificata mediante audit interni condotti almeno una volta l'anno secondo la Procedura Audit Interni, combinabili con gli audit del sistema ISO 14001, e mediante il riesame della direzione.

Il mancato rispetto della presente policy può comportare azioni correttive e, a seconda della gravità della violazione, provvedimenti disciplinari secondo il sistema disciplinare già adottato dall'organizzazione nell'ambito del Modello 231 e del CCNL applicabile, fino alla risoluzione del rapporto e, nei casi previsti, alla segnalazione alle autorità competenti. Per i fornitori e i collaboratori esterni si applicano le conseguenze previste dai rispettivi accordi contrattuali e di riservatezza.



Cavallermaggiore, 12/11/2026