Questo documento definisce la Politica di sicurezza delle informazioni di **CORIPET**.

Essere competitivi significa puntare a differenziare le caratteristiche dei propri servizi attraverso una costante ricerca volta al costante miglioramento continuo dell'efficacia e della efficienza dei processi aziendali sotto i punti di vista della qualità, delle prestazioni aziendali e della sicurezza delle informazioni.

CORIPET ritiene che la sicurezza delle informazioni rappresenti un fattore critico di successo sia per quanto riguarda i processi di pianificazione, coordinamento e monitoraggio delle attività correlate al recupero/riciclo degli imballaggi in PET per liquidi alimentari e relativi semilavorati e accessori di imballaggio intercettati tramite la raccolta differenziata e selettiva con eco compattatori, al fine del raggiungimento degli obiettivi normativi di avvio al riciclo di tale tipologia di imballaggi, ma anche per il processo dello sviluppo di iniziative di promozione e di informazione dirette a sensibilizzare gli utenti finali e ad incentivare la raccolta del PET, infine, anche per tutto ciò che riguarda l'erogazione dei servizi offerti ai propri clienti e stakeholder.

Per CORIPET la Gestione della Sicurezza delle Informazioni ha come <u>obiettivo primario</u> la protezione dei dati e delle informazioni al fine di tutelare il patrimonio rappresentato dalle conoscenze aziendali, quello dei propri clienti e di tutelare le persone fisiche di cui si trattano i dati personali.

Per le caratteristiche dei servizi che **CORIPET** offre ai propri clienti e per il valore che rappresentano le informazioni nel proprio business la Politica della Sicurezza delle Informazioni rappresenta un indirizzo strategico fondamentale e prioritario.

La Politica della Sicurezza delle Informazioni definisce e organizza la riservatezza, l'integrità e la disponibilità delle informazioni e gestisce tutti gli aspetti ad essa collegati, da quelli tecnici e tecnologici a quelli organizzativi e di business, a quelli sul controllo dell'attività dei collaboratori agli aspetti della sicurezza dei luoghi fisici dell'Organizzazione.

La Politica per la sicurezza delle informazioni per **CORIPET** è costituita da un insieme di attività che comprendono:

- l'identificazione delle aree critiche,
- la gestione dei rischi,
- dei sistemi e della rete,
- delle vulnerabilità e degli incidenti,
- il controllo degli accessi,
- la gestione della privacy e della compliance,
- la valutazione dei danni e tutti gli altri aspetti che possono impattare sulla gestione della sicurezza delle informazioni.

Per perseguire l'obiettivo sopracitato **CORIPET**, attraverso un approccio by design, pone grande attenzione alla progettazione, alla gestione e alla manutenzione della propria struttura tecnologica, fisica, logica ed organizzativa.

Pertanto, in qualità di azienda moderna e lungimirante, **CORIPET** riconosce la necessità di garantire che la propria attività operi senza intoppi e senza interruzioni a vantaggio dei propri clienti, azionisti e altre parti interessate.
Al fine di fornire un tale livello di funzionamento continuo, **CORIPET,** in linea con la propria mission, ha deciso di implementare un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) in linea con lo standard internazionale ISO/IEC 27001:2022. Questo standard definisce i requisiti per un SGSI basato sulle migliori pratiche riconosciute a livello internazionale.

Il corretto funzionamento dell'SGSI permette a **CORIPET** di conseguire molti vantaggi competitivi, tra cui:

- Tutela dei flussi di reddito e della redditività aziendale
- Garantire la fornitura di beni e servizi ai clienti
- Mantenimento e valorizzazione del valore per gli azionisti
- Conformità ai requisiti legali e normativi

CORIPET si impegna quindi, ed in particolare, impegna le proprie risorse a sviluppare e mantenere un Sistema di Gestione per la Sicurezza delle Informazioni nell'ambito delle attività svolte e dei servizi erogati al fine di garantire quanto segue:

- la **riservatezza** delle informazioni attraverso la definizione puntuale delle responsabilità interne per la gestione dei servizi e delle informazioni ad essi connesse; il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente;
- **l'integrità** delle informazioni attraverso il controllo degli accessi fisici e logici agli archivi elettronici e cartacei esclusivamente da parte di personale autorizzato e competente e la gestione dei back-up dei dati e delle configurazioni dei sistemi informativi;
- la **disponibilità** delle informazioni attraverso l'identificazione dei ruoli e delle funzioni, i diritti di accesso alle informazioni e agli asset aziendali per la gestione dei servizi al Cliente;
- che dipendenti, fornitori, partner, appaltatori e ogni altra terza parte coinvolta con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione della Sicurezza delle Informazioni, accettino gli **obblighi e le responsabilità** di propria pertinenza, al fine di proteggere le informazioni, i beni e le risorse di **CORIPET**;
- che ogni accesso, di tipo fisico o informatico, sia autorizzato, controllato e monitorato sulla base dei seguenti criteri:
    - (a) l'accesso è autorizzato al personale abilitato solo per le informazioni necessarie (principio della conoscenza minima o necessità di sapere);
    - (b) l'accesso è autorizzato al personale abilitato solo per le informazioni relative alle attività specifiche (funzione di lavoro-correlati);
    - (c) l'accesso alla struttura e ai locali è autorizzato al personale abilitato. L'accesso ai locali di **CORIPET** è autorizzato, controllato e monitorato in linea con la politica aziendale.
- che ogni dipendente, fornitore, imprenditore e terza parte sia **consapevole del proprio ruolo** e dell'impatto delle proprie azioni sulla sicurezza delle informazioni.
- che ogni risorsa riceva un adeguato livello di **formazione e addestramento** sulle politiche e sulle procedure relative alla gestione della sicurezza delle informazioni.
- che i trattamenti delle informazioni, delle attività, delle risorse e delle soluzioni inerenti la protezione delle informazioni di **CORIPET** o gestiti dalla stessa per conto dei propri clienti sono conformi alle leggi e ai regolamenti applicabili di natura cogente, contrattuale e volontaria.
- che ogni attività e risorsa di **CORIPET** o affidata da questa a terze parti, nonché ogni informazione pertinente l'ambito del SGSI, è protetta contro i problemi legati alla riservatezza, l'integrità e la disponibilità, in proporzione al loro valore e nel rispetto delle leggi vigenti.
- che tutto il personale **CORIPET** sia responsabilizzato all'obbligo di:
    - (a) garantire il rispetto delle norme, leggi e regolamenti vigenti, di natura cogente, contrattuale e volontaria rese applicabili negli ambiti del SGSI;
    - (b) proteggere la riservatezza, l'integrità e la disponibilità delle informazioni gestite da **CORIPET**, la proprietà intellettuale e il patrimonio di **CORIPET** o da questa affidati a terze parti;
    - (c) aver cura dei beni materiali, i sistemi e le risorse di **CORIPET**;
    - (d) salvaguardare e gestire in modo appropriato ogni informazione e dato afferenti le attività di propria competenza;
    - (e) contattare la Direzione, il Responsabile della Sicurezza delle informazioni e/o altre autorità competenti in caso di effettive o sospette violazioni della sicurezza;
    - (f) segnalare qualsiasi necessità di modifiche alle procedure relative alla gestione della sicurezza delle informazioni. Compatibilmente con le autorità assegnate nella gestione della sicurezza ciascuno deve:
    - (g) garantire la conformità con la politica di sicurezza, requisiti, standard e/o procedure definiti;
    - (h) individuare e definire i diritti di accesso agli assets per le loro specifiche attività e responsabilità;
    - (i) richiedere alle terze parti di essere formalmente in linea con gli accordi di riservatezza;
    - (l) operare in conformità ai livelli di rischio che sono stati definiti per il proprio ambito di pertinenza.
- che tutto il personale cui sono assegnate responsabilità specifiche nella gestione della sicurezza delle informazioni ha altresì il dovere di:

- (a) implementare la sicurezza sulla base delle politiche di sicurezza della **CORIPET**;
- (b) garantire e monitorare il rispetto delle politiche di sicurezza delle informazioni, requisiti, norme e procedure definiti da **CORIPET** nell'ambito del SGSI;
- (c) monitorare gli asset aziendali, al fine di garantire il rispetto del livello di controllo previsto per l'asset da proteggere ed il rispetto delle leggi e regolamenti applicabili;
- (d) rendere effettive l'insieme di regole, funzioni, strumenti, oggetti e controlli, resi coerenti e funzionali agli scopi dell'organizzazione e coerenti con gli ambiti del SGSI, che garantiscano che nella struttura, organizzazione, ambiente informatico, singolo elaboratore, sia costantemente osservato il rispetto dei requisiti del SGSI;
- (e) garantire che il personale di **CORIPET** e i terzi siano formati e informati sulla politica, i requisiti, linee guida, standard, procedure ed istruzioni operative per la gestione della sicurezza delle informazioni, nonché resi consapevoli delle conseguenze in caso di mancato rispetto della politica e requisiti stabiliti in tali ambiti;
- (f) sostenere l'adozione di misure adeguate a garantire il controllo sugli aspetti che hanno impatto sulla sicurezza delle informazioni;
- (g) contenere il livello di rischio negli ambiti di pertinenza;
- (h) mantenere attive le misure da adottarsi in caso di incidenti derivanti dal verificarsi di condizioni anomale e di emergenza, garantire l'adozione dei piani di continuità in conformità ai requisiti definiti dal SGSI.

- Inoltre, che i soggetti terzi che gestiscono in modo diretto o indiretto gli asset sensibili di **CORIPET** e dei Clienti, sono obbligati, nello svolgimento di processi/attività, a:
  - (a) formalizzare il proprio impegno alla riservatezza e non divulgazione delle informazioni tratte negli ambiti di competenza;
  - (b) proteggere le risorse e le informazioni fisiche e intellettuali a cui possono accedere nella effettuazione delle attività assegnate;
  - (c) garantire la piena osservanza ai requisiti del SGSI nei comportamenti e nell'operatività.

CORIPET ha deciso di ottenere la certificazione del proprio di sistema di gestione per la sicurezza delle informazioni secondo lo standard internazionale ISO/IEC 27001:2022, certificazione convalidata da una terza parte indipendente, un Organismo di Certificazione registrato il quale, attraverso ispezioni periodiche, verifica l'effettiva adozione delle migliori prassi per la sicurezza delle informazioni.

Questa politica si applica a tutti i sistemi, persone e processi che costituiscono i sistemi informativi dell'organizzazione, inclusi membri del consiglio di amministrazione, direttori, dipendenti, fornitori e altre terze parti che hanno accesso ai sistemi di **CORIPET**.

La **Direzione Generale**, da parte sua, si impegna a riesaminare periodicamente la propria Politica per la Sicurezza delle Informazioni per garantirne la continua idoneità.

Milano, 01/07/2023

La Direzione

(Giovanni Alberti)