# POLITICA DI SICUREZZA DELLE INFORMAZIONI

La politica della sicurezza delle informazioni mira a proteggere le informazioni da ogni possibile minaccia, interna o esterna, voluta o accidentale e descrive gli obiettivi, le strategie, i processi, i ruoli e le responsabilità messe in atto da Fives Intralogistics S.p.A. per garantire gli aspetti di riservatezza, integrità e disponibilità a tutti i soggetti coinvolti: clienti, fornitori, partner, dipendenti e collaboratori.

La politica di sicurezza è ispirata agli standard ISO 27001 e al Regolamento UE 2016/679 (GDPR). In particolare è utilizzata come riferimento delle pratiche operative la ISO 27002, raccolta di "best practices" che possono essere adottate per soddisfare i requisiti della norma ISO 27001 al fine di proteggere le risorse informative.

I dati, le informazioni e conseguentemente le applicazioni e i sistemi che li trattano, soprattutto quelli che rivestono una valenza strategica per il business aziendale, sono protetti con sistemi di sicurezza commisurati al loro valore e ai rischi a cui sono sottoposti. In tale contesto sono definiti "asset" le risorse aziendali materiali ed immateriali che necessitano di protezione per il loro valore di business.

La politica della sicurezza delle informazioni si basa su principi di base e requisiti di protezione che sono garantiti attraverso un insieme di procedure per il trattamento degli asset nell'ambito dei processi di business (sicurezza logica) e un contesto adeguato ove tali processi avvengono (sicurezza fisica).

I principi alla base della politica della sicurezza delle informazioni sono:

- La sicurezza degli asset (sistemi, applicazioni, apparati di rete e dati) è un prerequisito per ogni processo di business svolto dall'azienda e deve coinvolgere i clienti, fornitori, partner, dipendenti e collaboratori;
- La protezione è adeguata quando sono garantiti gli aspetti di riservatezza, integrità e disponibilità degli asset e il rischio di violazioni è evitato o può essere ridotto in modo accettabile;
- Tutti i dipendenti sono responsabili dell'implementazione del sistema di sicurezza delle informazioni e devono quindi essere informati e periodicamente aggiornati sulle procedure a cui attenersi;
- Ciascun asset aziendale ha un responsabile formale che provvede alla identificazione e classificazione dell'asset nonché alla definizione dei requisiti di protezione in relazione al rischio a cui sono esposti;
- Tutti gli utenti sono identificati e autorizzati prima di avere accesso agli asset e le informazioni devono essere protette da accessi non autorizzati;
- I diritti di accesso agli asset vengono stabiliti dal responsabile sulla base dei principi "need to know" (accesso alle informazioni strettamente necessarie allo svolgimento del compito assegnato), "least privilege" (accesso alle informazioni limitato con il minimo privilegio

necessario per il compito assegnato), "separation of duties" (autorizzazione ed esecuzione devono essere in carico a persone differenti);

- I diritti di accesso sono limitati in termini di ambito sulla base del profilo assegnato per ciascun utente
- I diritti di accesso sono immediatamente modificati o rimossi in funzione dei cambiamenti di ruolo dell'utente e del termine del rapporto di collaborazione;
- Gli accessi e le attività sono tracciate al fine di rilevare l'utente che ha eseguito l'operazione e quando è avvenuta; la raccolta di queste informazioni avviene nel rispetto dei Regolamenti e delle leggi in vigore;
- Le leggi, i regolamenti ed i contratti afferenti alla sicurezza informativa sono ottemperati;
- La sicurezza fisica, logica ed ambientale è garantita;
- Ogni violazione, accertata o presunta, del sistema di sicurezza delle informazioni è tempestivamente segnalata, indagata e documentata;
- Tutte le infrazioni della politica della sicurezza delle informazioni sono sanzionate.

Lonate Pozzolo, Settembre 2018

Lorenzo Moroni
Chief Executive Officier