Politica della Direzione
Sistema di Gestione Integrato

ELPE GLOBAL LOGISTIC SERVICES S.P.A. ha adottato e applica un Sistema di Gestione Integrato (SGI) ai sensi delle norme internazionali ISO 9001 (Qualità), ISO 45001 (Sicurezza sul Lavoro), ISO 14001 (Gestione Ambientale), ISO 37001 (Prevenzione della Corruzione), ISO 27001 (Sicurezza dei dati e delle informazioni).

ELPE assume così l'impegno a garantire la qualità nella progettazione, pianificazione e realizzazione dei servizi erogati ai propri clienti e la sicurezza e il benessere delle proprie risorse che partecipano al raggiungimento degli obiettivi comuni.

ELPE concepisce il proprio SGI in via preliminare come leva organizzativa per pianificare e monitorare il corretto funzionamento dei processi necessari al perseguimento degli obiettivi definiti dalla Direzione attraverso le attività svolte da lavoratori/trici: pertanto un ambiente di lavoro sicuro e organizzato e l'adozione di prassi finalizzate a contenere quanto più possibile gli impatti ambientali sono componenti fondamentali della mission aziendale.

Inoltre, pienamente consapevole che il fenomeno della corruzione rappresenta un ostacolo allo sviluppo economico, politico e sociale di un Paese e una pesante distorsione delle regole, della correttezza e della competitività dei mercati, ***ELPE*** ha definito prassi atte a tenere sotto controllo il fenomeno corruttivo, anche mediante una formazione costante delle proprie risorse e il coinvolgimento dei soci in affari.

ELPE garantisce le risorse (persone, budget, strumenti) adeguate e necessarie per monitorare costantemente i rischi connessi alla gestione dei dati e delle informazioni e definisce e comunica con chiarezza i ruoli, le responsabilità e le autorità necessarie.

I principi ispiratori del modo di operare di ***ELPE*** comprendono attitudini quali la volontà di porre sempre il cliente al centro del proprio interesse, l'attenzione costante al rispetto dei Diritti Umani e alla sicurezza nei luoghi di lavoro oltre che alla tutela ambientale, l'abitudine al confronto interno ed esterno sulle best practices, la costante ricerca del miglioramento.

I molteplici elementi che ***ELPE*** ritiene vincenti nel proprio modo di operare sono:

- la capacità di individuare in modo proattivo i reali bisogni dei clienti sia attivi che potenziali, ovvero la capacità di raccogliere le esigenze, interpretarle e indirizzarle nel modo più efficace fornendo le risorse necessarie a garantire un'adeguata gestione dei servizi richiesti;
- la flessibilità operativa della struttura, che permette di cogliere le opportunità di lavoro ritenute più interessanti;
- l'effettuazione di accurate analisi dei contesti lavorativi ove opera al fine di identificare, nell'ambito delle attività svolte, le aree di pericolo potenziale e così individuare e attuare azioni idonee a ridurre e minimizzare i rischi stessi;
- la capacità di organizzare i processi e standardizzare le attività attraverso la definizione di prassi specifiche e sistematiche e il continuo aggiornamento e implementazione di un sistema informativo adeguato a supporto degli obiettivi aziendali;
- un approccio metodologico basato sulla misurazione delle prestazioni e in cui le decisioni strategiche sono guidate dalla valutazione e dal trattamento dei rischi incentrati sul concetto per cui i rischi non accettabili vanno gestiti prioritariamente e i rischi accettabili sono formalizzati
- la definizione periodica di piani di miglioramento, sia per quanto riguarda il proprio business che per ogni aspetto concernente la sicurezza degli ambienti di lavoro, la tutela della salute e la riduzione degli impatti ambientali al fine di minimizzare, ove tecnicamente possibile ed economicamente sostenibile, ogni impatto negativo sull'ambiente;
- il contatto continuo con i clienti, veri "certificatori" della qualità del servizio fornito;
- il rispetto, nei contenuti e nei principi, dei Diritti Umani in generale e, in particolare, delle norme di legge in materia di sicurezza e igiene applicabili ai servizi erogati;
- il rigoroso e pieno rispetto della legislazione vigente in materia di prevenzione e contrasto alla corruzione, in Italia e in qualsiasi Paese dove si dovesse trovare ad operare, con il coinvolgimento di dipendenti, collaboratori a qualsiasi titolo e di tutti i soggetti che operano a favore e/o sotto il suo controllo;

- l'attuazione di azioni di coordinamento e cooperazione con committenti e fornitori al fine di promuovere ogni iniziativa volta a prevenire l'accadimento di incidenti che possano compromettere la sicurezza di lavoratori e lavoratrici o che possano favorire lo sviluppo di fenomeni corruttivi;
- la volontà, ove possibile, di applicare volontariamente tutti i provvedimenti ritenuti utili, anche in assenza di obblighi legislativi, al fine di innalzare il livello di sicurezza negli ambienti di lavoro;
- la designazione di una funzione di conformità per la prevenzione della corruzione, cui viene garantita piena autorità e indipendenza nell'incarico;
- il divieto assoluto di attuare comportamenti che possano configurarsi come corruzione o tentativo di corruzione;
- il perseguimento di qualsiasi comportamento non conforme alla politica per la prevenzione della corruzione con l'applicazione del sistema sanzionatorio;
- l'attività di sensibilizzazione presso i soci in affari perché adottino, nelle attività di specifica competenza, politiche e azioni per la prevenzione dei fenomeni corruttivi, rispettose delle prescrizioni di legge e coerenti con gli obiettivi aziendali;
- la pianificazione e attuazione di piani di formazione e addestramento del personale sia sulle prassi operative che di sensibilizzazione alle tematiche:
  - della sicurezza sul lavoro,
  - dell'impatto ambientale delle attività svolte (raccolta differenziata dei rifiuti, consumo consapevole delle materie prime, corretta gestione dell'operazione di stoccaggio di sostanze potenzialmente pericolose, ecc.)
  - della prevenzione del fenomeno corruttivo.
- la presenza di una struttura di supervisione e controllo competente e organizzata in modo tale da produrre reportistica in grado di garantire un monitoraggio costante sia del livello di servizio reso e percepito, sia dei dati relativi ai processi interni, sia dei dati connessi all'impatto ambientale, come quelli, ad esempio, relativi ai consumi idrici ed energetici.

In ambito Sicurezza delle informazioni la Direzione di ***ELPE***:

- adotta una logica di minimo privilegio: gli accessi sono concessi solo se necessari e limitati al minimo;
- adotta un approccio di "difesa in profondità" con controlli multilivello (organizzativi, fisici, tecnici) per ridurre l'impatto di eventuali compromissioni;
- adotta la logica di sicurezza by design e by default: requisiti di sicurezza integrati in processi, progetti e sviluppo software;
- garantisce il rispetto di obblighi legali, regolatori e contrattuali (es. GDPR, licenze software, accordi clienti/fornitori);

Lavoratori, lavoratrici e tutti i soggetti coinvolti nelle attività di ***ELPE*** sono incoraggiati a segnalare ogni situazione di cui abbiano conoscenza, anche indiretta, che possa costituire una violazione dei Diritti Umani o compromettere la salute delle risorse, configurare un rischio dal punto di vista ambientale o una violazione del sistema di prevenzione della corruzione.
Ai/alle segnalanti è garantita tutela da qualsiasi forma di ritorsione, discriminazione o penalizzazione, fatti salvi gli obblighi di legge.

È soggetto/a a sanzione disciplinare, commisurata alla gravità della violazione effettuata, qualsiasi dipendente o collaboratore/trice che non agisca conformemente alla presente Politica.
È soggetto a sanzioni disciplinari di tipo contrattuale qualsiasi partner o fornitore che non agisca conformemente alla presente Politica.

Torino, 16 aprile 2026

LA DIREZIONE

1. Scopo

La presente Politica definisce i principi e gli impegni di Elpe Global Logistic Services S.p.a. per proteggere le informazioni e i servizi che le trattano, assicurando **riservatezza, integrità e disponibilità** (CIA - Confidentiality, Integrity and Availability) e supportando l'implementazione e il miglioramento continuo del **Sistema di Gestione per la Sicurezza delle Informazioni** (ISMS - Information Security Management System) in conformità alla norma ISO/IEC 27001.

2. Ambito di applicazione

La Politica si applica a tutte le **informazioni,** in qualsiasi formato (**digitale, cartaceo, verbale**), ai **sistemi informativi, a infrastrutture, reti, applicazioni, dispositivi** (aziendali e personali ove consentito –BYOD -Bring Your Own Device) e a tutto il **personale**, dipendenti e consulenti, nonché a **fornitori e terze parti** che operano entro il perimetro definito dallo Scopo del ISMS.

3. Principi generali

- Approccio basato sul rischio: le decisioni sono guidate dalla valutazione e dal trattamento dei rischi.
- Minimo privilegio e need-to-know: gli accessi sono concessi solo se necessari e sono limitati al minimo.
- Difesa in profondità: controlli multilivello, organizzativi, fisici e tecnici riducono l'impatto di eventuali compromissioni.
- Responsabilità e tracciabilità: ruoli chiari, registrazioni e logging adeguati per attribuire azioni e supportare audit.
- Sicurezza by design e by default: requisiti di sicurezza integrati in processi, progetti e sviluppo software.
- Conformità: rispetto di obblighi legali, regolatori e contrattuali (es. GDPR, licenze software, accordi clienti/fornitori).
- Miglioramento continuo: misurazione delle prestazioni del Sistema e attivazione di azioni correttive/preventive.

4. Obiettivi della sicurezza delle informazioni

ELPE definisce e mantiene obiettivi misurabili di sicurezza delle informazioni coerenti con la strategia aziendale.

5. Impegni della Direzione

- Approvare la presente Politica e sostenerne l'applicazione a tutti i livelli dell'Organizzazione.
- Assicurare risorse adeguate (persone, budget, strumenti) per l'attuazione e il mantenimento del Sistema.
- Garantire che ruoli, responsabilità e autorità siano assegnati e comunicati chiaramente.
- Promuovere la cultura della sicurezza delle informazioni.
- Assicurare che i rischi non accettabili siano trattati con priorità.

6. Ruoli e responsabilità

La responsabilità della sicurezza delle informazioni è condivisa. In particolare:

- Direzione: definisce l'indirizzo strategico, approva Politica, obiettivi e accettazione dei rischi significativi.
- Responsabile ICT: governa l'ISMS, coordina risk assessment/trattamento, controlli e miglioramento continuo.
- Amministratori: implementano e gestiscono i controlli tecnici (hardening, accessi, logging, backup, patching).
- Addetti Ufficio IT: classificano gli asset, definiscono requisiti e autorizzano accessi.
- DPO: presidia aspetti privacy e protezione dei dati personali e interazioni con GDPR.
- HR / Formazione: supporta onboarding/offboarding, formazione e consapevolezza, misure disciplinari ove necessario.
- Utenti: rispettano policy e procedure, proteggono credenziali e segnalano tempestivamente eventi sospetti.
- Fornitori / Terze parti: rispettano requisiti contrattuali di sicurezza, inclusa notifica di eventuali incidenti.

7. Regole essenziali di protezione

Le regole operative dettagliate sono definite in procedure e istruzioni specifiche.

A livello di principio, l'Organizzazione assicura almeno:

- Gestione degli asset tramite l'aggiornamento di un inventario.
- Controllo accessi: identity lifecycle, MFA ove applicabile, revisione periodica privilegi e segregazione dei compiti.
- Protezione endpoint e sistemi: hardening, patch management, anti-malware / EDR, configurazioni sicure e change management.

- Sicurezza di rete: segmentazione, firewalling, VPN per accessi remoti, monitoraggio e protezione dei servizi di rete.
- Logging e monitoraggio: raccolta eventi rilevanti, integrità e retention dei log, alerting per anomalie.
- Backup e ripristino: backup regolari, protezione delle copie, test periodici di restore automatici e definizione RTO / RPO ove applicabili.
- Gestione degli incidenti: canali di segnalazione, escalation, contenimento, ripristino e lesson learned.
- Gestione fornitori e cloud: requisiti di sicurezza contrattuali, valutazione rischio, monitoraggio e offboarding sicuro.
- Protezione dei dati personali: minimizzazione, access control, cifratura, retention e gestione data breach secondo GDPR.

8. Conformità, eccezioni e misure disciplinari

La conformità a questa Politica e alle procedure correlate è obbligatoria. Eventuali eccezioni devono essere motivate, valutate in termini di rischio, approvate dal Responsabile ICT (e dalla Direzione se rilevanti) e registrate. Violazioni possono comportare misure correttive e disciplinari, oltre ad azioni tecniche di contenimento.

9. Comunicazione, formazione e consapevolezza

ELPE assicura che il personale riceva formazione iniziale e periodica, e che siano svolte attività di awareness (es. campagne phishing, linee guida operative).
Il documento della Politica è comunicato e reso disponibile alle parti interessate pertinenti, incluse terze parti quando applicabile.

10. Monitoraggio, audit e riesame

L'efficacia dell'ISMS è verificata tramite Indicatori, audit interni, controlli periodici e riesami della Direzione.

Torino, 5 Maggio 2026

LA DIREZIONE