POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	09/06/2026	Alessandra Zanoli	MARINA ALEJANDRA DI DONATO

Indice

Scopo

La presente politica dichiara e comunica l'impegno del Top Management di K.E. Group of Company Srl verso la protezione degli asset informativi dell'organizzazione. Attraverso questo documento, la Direzione definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), con l'obiettivo di preservare la riservatezza, l'integrità e la disponibilità delle informazioni che supportano le attività di realizzazione di impianti elettrici, di condizionamento e termoidraulici, i lavori di ristrutturazione di edifici civili e industriali e i servizi di gestione pratiche come general contractor.

L'organizzazione riconosce che la sicurezza delle informazioni costituisce un fattore critico per la tutela della propria reputazione, la continuità operativa e il rispetto degli obblighi contrattuali verso clienti pubblici e privati. Con la presente politica, K.E. Group of Company Srl si impegna a garantire che il SGSI rimanga appropriato al contesto aziendale, orientato al soddisfacimento dei requisiti applicabili e al miglioramento continuo delle proprie prestazioni in materia di sicurezza delle informazioni.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di K.E. Group of Company Srl, inclusi i sistemi informatici (Microsoft 365, server aziendale, gestionale Blade), le repository documentali (OneDrive, Server, Blade) e le informazioni gestite in formato cartaceo e digitale. L'ambito comprende la sede legale di Via Zara 2, Romano di Lombardia (BG) e la sede operativa di Via Marco Biagi, Fara Olivana Con Sola (BG).

Sono destinatari della politica tutti i dipendenti, i collaboratori a contratto, i fornitori e le terze parti che accedono alle informazioni o ai sistemi aziendali. Restano esclusi dal presente documento gli aspetti relativi al lavoro da remoto, in quanto l'organizzazione non effettua tale modalità lavorativa.

Riferimenti normativi

- ISO/IEC 27001:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per la quale l'informazione non è resa disponibile o divulgata a individui, entità o processi non autorizzati.

- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione delle conseguenze di un evento e della relativa probabilità di accadimento.
- **Evento di sicurezza delle informazioni** : occorrenza identificata di uno stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza delle informazioni, un fallimento delle contromisure o una situazione precedentemente sconosciuta che può essere rilevante per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Asset** : qualsiasi elemento che abbia valore per l'organizzazione, inclusi informazioni, software, hardware, servizi e persone.

Ruoli e responsabilità

- **Dirigente** : approva la presente politica, assicura le risorse necessarie al SGSI e promuove la cultura della sicurezza delle informazioni a tutti i livelli dell'organizzazione.
- **Responsabile del sistema di gestione** : coordina l'attuazione e il mantenimento del SGSI, supervisiona il riesame periodico della politica e riferisce alla Direzione sulle prestazioni in materia di sicurezza delle informazioni.
- **Ufficio Amministrativo** : garantisce la corretta gestione della documentazione del SGSI e supporta la comunicazione della politica agli stakeholder interni ed esterni.
- **Ufficio Acquisti** : verifica che i requisiti di sicurezza delle informazioni siano integrati nei rapporti con fornitori, appaltatori e terze parti.
- **Architetto** : assicura che i requisiti di sicurezza delle informazioni siano considerati nella progettazione e gestione dei progetti.

Obiettivi di sicurezza delle informazioni

K.E. Group of Company Srl persegue i seguenti obiettivi strategici di sicurezza delle informazioni, coerenti con il proprio contesto organizzativo e con gli indirizzi del sistema di gestione:

- **Protezione del patrimonio informativo** : l'organizzazione si impegna a salvaguardare la riservatezza, l'integrità e la disponibilità di tutte le informazioni aziendali — dai dati tecnici di progetto alla documentazione amministrativa e contrattuale — attraverso misure organizzative e tecniche proporzionate al valore degli asset e ai rischi identificati.
- **Gestione proattiva dei rischi** : l'organizzazione adotta un approccio sistematico all'identificazione, alla valutazione e al trattamento dei rischi per la sicurezza delle informazioni, con l'obiettivo di mantenere il livello di rischio residuo entro soglie accettabili, definite nel processo di valutazione dei rischi.

- **Conformità normativa e contrattuale** : l'organizzazione si impegna a soddisfare i requisiti legali, regolamentari e contrattuali applicabili alla protezione delle informazioni, con particolare riguardo alla normativa sulla protezione dei dati personali e agli impegni assunti verso clienti pubblici e privati nell'ambito di appalti e commesse.
- **Consapevolezza e competenza del personale** : l'organizzazione promuove la sensibilizzazione e la formazione continua di tutto il personale in materia di sicurezza delle informazioni, affinché ogni collaboratore comprenda il proprio ruolo nella protezione degli asset informativi e agisca in conformità alle politiche e procedure del SGSI.
- **Miglioramento continuo** : l'organizzazione si impegna a misurare le prestazioni del SGSI mediante indicatori adeguati, a riesaminare periodicamente l'efficacia dei controlli e ad avviare azioni correttive e preventive per elevare progressivamente il livello di protezione delle informazioni.

Principi fondamentali di sicurezza delle informazioni

K.E. Group of Company Srl fonda il proprio Sistema di Gestione della Sicurezza delle Informazioni su principi che orientano ogni decisione, comportamento e misura di protezione adottata dall'organizzazione.

Approccio basato sul rischio

L'organizzazione riconosce che la protezione delle informazioni richiede un'analisi sistematica delle minacce e delle vulnerabilità che possono compromettere la sicurezza degli asset informativi. Ogni decisione relativa all'adozione di controlli è guidata dalla valutazione del rischio, che considera la probabilità di accadimento e l'impatto potenziale sugli obiettivi aziendali. Questo approccio consente di allocare le risorse in modo proporzionato e di trattare prioritariamente i rischi che superano le soglie di accettabilità stabilite dalla Direzione.

Responsabilità condivisa

La sicurezza delle informazioni non è una responsabilità esclusiva di una singola funzione, ma un impegno che coinvolge l'intera organizzazione. Ogni persona che accede alle informazioni o ai sistemi aziendali — dipendente, collaboratore o terza parte — è tenuta a contribuire attivamente alla protezione degli asset informativi nell'ambito delle proprie mansioni. L'organizzazione promuove una cultura in cui la segnalazione tempestiva di anomalie e potenziali minacce è riconosciuta come un contributo essenziale alla sicurezza collettiva.

Uso accettabile delle informazioni e delle risorse

L'organizzazione stabilisce regole chiare per l'utilizzo delle informazioni e delle risorse associate, affinché ogni asset sia impiegato esclusivamente per finalità lavorative autorizzate. Al momento dell'assegnazione, i beni aziendali — PC portatili, smartphone, account e-mail, credenziali software, badge e chiavi — sono consegnati mediante il *MOD Modulo di assegnazione dei beni* , e il consegnatario si impegna a custodirli con diligenza e

a restituirli alla cessazione del rapporto o su richiesta dell'organizzazione. L'accesso alle informazioni è limitato agli utenti formalmente autorizzati, sulla base del principio di necessità operativa, e gli accessi sono documentati e periodicamente riesaminati.

Scrivania pulita e schermo pulito

L'organizzazione adotta il principio della scrivania pulita e dello schermo pulito per prevenire l'accesso non autorizzato alle informazioni nei locali aziendali. I documenti contenenti informazioni riservate o limitate non sono lasciati incustoditi sulle scrivanie al termine dell'attività lavorativa, ma riposti in contenitori chiusi a chiave. Le postazioni di lavoro sono configurate con un blocco automatico dello schermo dopo un periodo di inattività di dieci minuti, e il personale attiva manualmente il blocco ogni volta che si allontana dalla propria postazione. L'efficacia di queste misure è verificata attraverso test periodici di sicurezza fisica.

Segnalazione degli eventi di sicurezza delle informazioni

L'organizzazione fornisce a tutto il personale un meccanismo chiaro e accessibile per segnalare tempestivamente eventi di sicurezza delle informazioni osservati o sospetti. Ogni persona che rileva o sospetta un evento — quale accesso non autorizzato, perdita di dati, comportamento anomalo di un sistema o smarrimento di un dispositivo — è tenuta a comunicarlo senza ritardo al **Responsabile del sistema di gestione** utilizzando i canali di comunicazione interni (e-mail, telefono o segnalazione diretta). La segnalazione attiva il processo di gestione degli incidenti, e ciascun evento è registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni* per garantire tracciabilità e analisi successiva. L'organizzazione promuove un ambiente privo di ritorsioni nei confronti di chi segnala in buona fede, riconoscendo la tempestività della segnalazione come fattore critico per limitare gli impatti di un potenziale incidente.

Classificazione e protezione delle informazioni

L'organizzazione adotta un sistema di classificazione delle informazioni che distingue tre livelli — public, limited e confidential — ciascuno associato a requisiti di trattamento, trasmissione e conservazione proporzionati alla sensibilità del dato. Questo principio assicura che le misure di protezione siano commisurate al valore dell'informazione e al danno che la sua compromissione potrebbe causare.

Conformità e miglioramento continuo

L'organizzazione è impegnata a operare in conformità ai requisiti legali, regolamentari e contrattuali applicabili, nonché agli standard internazionali adottati. Le politiche e le procedure del SGSI sono soggette a riesame pianificato e ad aggiornamento in caso di cambiamenti significativi nel contesto operativo, nel panorama delle minacce o nella normativa di riferimento, in una logica di miglioramento continuo che rafforza progressivamente la postura di sicurezza dell'organizzazione.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione della Sicurezza delle Informazioni. Il **Responsabile del sistema di gestione** ne cura l'archiviazione all'interno del sistema documentale aziendale e ne assicura la disponibilità a tutto il personale interessato. La politica è sottoposta a riesame con cadenza annuale, in occasione del riesame di Direzione, o anticipatamente qualora intervengano cambiamenti significativi nell'organizzazione, nell'infrastruttura tecnologica, nel contesto normativo o nel panorama delle minacce. Le modifiche sono approvate dal **Dirigente** e comunicate agli stakeholder interni mediante i canali di comunicazione stabiliti e agli stakeholder esterni tramite pubblicazione sul sito web aziendale e comunicazione via e-mail.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione dei rischi
- PRO Procedura di configurazione, gestione e smaltimento degli asset