La GECAL SPA è un'organizzazione che ha come obiettivo di fornire alla clientela una consulenza professionale ed efficiente in un mondo in continua evoluzione, adottando comportamenti e processi improntati al rispetto e all'ottimizzazione delle risorse. Da oltre trent'anni "Daily Business Efficiency" è la nostra mission. Ogni giorno continuiamo a perseguirla, con la consapevolezza che le nostre soluzioni debbano essere sempre più sostenibili.

VALORI:

Integrità: orgogliosi di essere un gruppo di persone corrette e leali; Trasparenza: sinceri e chiari verso tutti gli interlocutori; Responsabilità personale: impegnati per il bene dell'Ambiente e dell'Azienda insieme; Coerenza: concentrati nel fare ciò che ci si prefigge.

OBIETTIVI DI MIGLIORAMENTO:

La Direzione è impegnata nel processo di responsabilizzazione delle risorse e verificherà periodicamente e regolarmente (o in concomitanza di cambiamenti significativi normativi e organizzativi) l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni, riesaminando la politica ed aggiornando l'analisi dei rischi sulle informazioni al fine di individuare e adottare le opportune azioni migliorative. L'impegno della direzione si concretizza tramite una struttura organizzativa i cui compiti sono:

- garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni in aderenza con le politiche e le strategie della società;
- dotarsi di un approccio sistematico per l'analisi del rischio sulle informazioni;
- ridurre al minimo la probabilità e gli impatti derivanti da incidenti sulla sicurezza delle informazioni;
- incrementare, in un'ottica di "accountability", i livelli di sicurezza nel trattamento dei dati personali;
- favorire un'efficace integrazione tra i requisiti di sicurezza delle informazioni e i requisiti obbligatori della normativa italiana (D. Lgs. 196/2003 armonizzato con il D. Lgs. 101/2018) ed europea (Regolamento UE 2016/679) sul trattamento dei dati personali;
- fornire risorse sufficienti per la pianificazione, implementazione, controllo e miglioramento continuo del SGSI;
- definire i ruoli e le responsabilità aziendali per la progettazione, miglioramento e mantenimento del SGSI;
- monitorare le prestazioni del SGSI e assicurare un sistema di risposta veloce ed efficacie nella gestione degli incidenti sulla sicurezza delle informazioni;
- monitorare i cambiamenti dell'esposizione alle minacce, rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- garantire programmi di informazione, sensibilizzazione e formazione del personale creando una cultura aziendale sulla sicurezza delle informazioni;
- definire procedure, istruzioni operative e linee guida comportamentali per assicurare la riservatezza, integrità e disponibilità delle informazioni;
- eseguire audit periodici per verificare il rispetto dei requisiti del SGSI.

Affinché ciò sia possibile, è necessario che tutta l'organizzazione conosca e condivida la Politica per la Sicurezza delle Informazioni. I principi base cui si basa la nostra politica sulla sicurezza delle informazioni comprendono i seguenti principi cardini:

- la conformità ai requisiti legislativi e le normative legate la sicurezza delle informazioni;
- la continua comunicazione, sensibilizzazione e formazione del personale al fine di favorire la consapevolezza e la conoscenza interna sull'importante e strategica tematica della sicurezza delle informazioni;
- l'adozione di un disciplinare informatico interno contenente le linee guida da rispettare in merito al corretto trattamento delle informazioni con modalità telematiche;
- un puntuale censimento e identificazione degli asset aziendali (le informazioni strategiche trattate e gli strumenti utilizzati per i trattamenti);

- l'adozione di un sistema di classificazione delle informazioni;
- l'adozione di un sistema di identificazione, analisi e trattamento dei rischi sulla sicurezza delle informazioni;
- un continuo bilanciamento di interessi tra l'esigenza di condividere la conoscenza all'interno della società e l'esigenza di garantire la sicurezza delle informazioni; in tal senso la sicurezza delle informazioni non deve pregiudicare l'efficienza e lo scambio di conoscenza come valore aggiunto nella gestione dei progetti;
- la definizione di chiare e vincolanti clausole contrattuali e accordi di riservatezza sulla sicurezza delle informazioni con i collaboratori, fornitori e i clienti della società;
- il rispetto di procedure e sistemi di controllo atti a prevenire l'accesso alle informazioni da parte di terzi non autorizzati;
- l'adozione di un sistema reattivo di gestione degli incidenti sulla sicurezza delle informazioni perfettamente integrato con il processo del Data Breach;
- l'attuazione di misure idonee di sicurezza informatiche per garantire: la protezione da codici malevoli (antivirus), la disponibilità delle informazioni (backup & recovery) e la riservatezza delle informazioni (firewall, intrusion prevention system, logging, crittografia, ecc.);
- la predisposizione di piani di disaster & recovery e business continuity per favorire la continuità operativa in caso di eventi bloccanti imprevisti, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino il più possibile le conseguenze negative;
- la predisposizione di procedure aziendali per lo sviluppo sicuro del software;
- la predisposizione di strumenti di monitoraggio, controllo e audit Interni per verificare il rispetto degli obiettivi prefissati sulla sicurezza delle informazioni e delle disposizioni della normativa ISO 27001;
- la promozione di programmi di miglioramento continui del sistema di gestione per la sicurezza delle informazioni.

A tal fine l'azienda si è dotata di un sistema di gestione della sicurezza delle informazioni (SGSI) che in accordo con i principi sopraelencati e con lo scopo di contenere tali rischi a livelli accettabili e di risultare competitivi nei costi prevede il raggiungimento dei seguenti obiettivi:

- essere conformi alle normative di legge (a titolo esemplificativo e non esaustivo, al D.Lgs. 196/03, al Regolamento UE 2016/679, ed al D.Lgs. 231/01), agli standard e regolamenti di settore e ai requisiti contrattuali della Clientela;
- mantenere un sistema di sicurezza aziendale allineato a buone pratiche e standard internazionali, dandone evidenza alle parti interessate;
- verificare, mediante un processo di valutazione e gestione del rischio, il continuo allineamento strategico degli obiettivi di sicurezza con il business aziendale;
- diffondere in Azienda una cultura della sicurezza delle informazioni;
- considerare il miglioramento continuo quale pratica per il mantenimento di un adeguato livello di sicurezza.

La Direzione dell'azienda condivide i Principi e gli Obiettivi per la Sicurezza delle Informazioni sopra descritti e supporta pienamente un programma per la loro attuazione e mantenimento.

La Direzione dell'azienda approva ed emette il presente documento di Politica, quale documento

In questo contesto nasce l'impegno di **GECAL SPA** a mantenere e migliorare costantemente l'efficacia e l'adeguatezza di un sistema di gestione aziendale adatto alla evoluzione del nostro business, frutto della fusione e del rispetto dei requisiti individuati nella norma internazionale ISO/IEC 27001:2022.

Paderno Dugnano, 25/09/2025

La Direzione: _____