POLITICA AZIENDALE DI GRUPPO PER LA SICUREZZA DELLE INFORMAZIONI

SCOPO E OBIETTIVI

DALE CONSULTING, in linea con la propria mission aziendale, adotta un approccio sistemico alla gestione della sicurezza delle informazioni, conforme alla norma ISO/IEC 27001:2022.

La presente politica ha l'obiettivo di:

- Proteggere le informazioni aziendali da minacce interne o esterne, accidentali o intenzionali;
- Garantire la riservatezza, l'integrità e la disponibilità delle informazioni;
- Promuovere una cultura della sicurezza diffusa a tutti i livelli organizzativi.

La direzione si impegna a mantenere attiva, aggiornata e condivisa questa politica in tutta l'organizzazione.

CAMPO DI APPLICAZIONE

La politica si applica a:

- Tutto il personale di DALE CONSULTING;
- Collaboratori esterni e soggetti terzi coinvolti nel trattamento delle informazioni;
- Tutti i processi, le sedi e i sistemi informativi aziendali.

L'applicazione della politica è obbligatoria e vincolante.
Ogni accordo con soggetti esterni deve includere il rispetto delle disposizioni in materia di sicurezza delle informazioni.
La comunicazione esterna delle informazioni è consentita solo se necessaria alle attività aziendali e in conformità con leggi e regolamenti vigenti.

PRINCIPI DI SICUREZZA

DALE CONSULTING si impegna a tutelare il proprio patrimonio informativo, assicurando:

- Riservatezza: le informazioni sono accessibili solo a chi è autorizzato;
- Integrità: le informazioni sono accurate, complete e protette da modifiche non autorizzate;
- Disponibilità: le informazioni sono accessibili quando necessario dagli utenti autorizzati.

Al fine di evitare che una carenza nella sicurezza possa comportare danni reputazionali, insoddisfazione dei clienti, sanzioni normative e perdite economiche.
La sicurezza è anche condizione necessaria per una gestione efficace delle informazioni condivise.

ANALISI E GESTIONE DEI RISCHI

L'azienda identifica le esigenze di sicurezza attraverso un'analisi dei rischi, valutando:

- Minacce e vulnerabilità del sistema informativo;
- Impatti potenziali dovuti alla mancata protezione;
- Probabilità di accadimento degli eventi avversi.

Sulla base dei risultati, vengono definite azioni correttive e misure di sicurezza adeguate a ridurre i rischi a un livello accettabile.

RESPONSABILITÀ

Tutti i dipendenti e collaboratori, interni ed esterni, sono tenuti a:

- Rispettare le regole definite nella presente politica;
- Segnalare tempestivamente anomalie, violazioni o comportamenti non conformi.

Il Responsabile del Sistema di Gestione ha il compito di:

- Condurre l'analisi dei rischi e definire le misure di gestione;
- Stabilire norme e procedure per una conduzione sicura delle attività;
- Monitorare violazioni e minacce, adottando contromisure;
- Promuovere formazione e sensibilizzazione del personale;
- Verificare periodicamente l'efficacia del sistema.

Ogni violazione intenzionale o dovuta a negligenza potrà essere oggetto di provvedimenti disciplinari o legali, nel rispetto delle normative e dei contratti vigenti.

IMPEGNO DELLA DIREZIONE

La Direzione garantisce un supporto attivo e continuativo alla sicurezza delle informazioni, attraverso:

- Definizione degli obiettivi di sicurezza coerenti con i requisiti aziendali;
- Assegnazione di ruoli e responsabilità specifiche per il SGSI;
- Allocazione di risorse adeguate alla pianificazione, implementazione e miglioramento continuo;
- Integrazione del SGSI in tutti i processi aziendali;
- Approvazione e sostegno delle iniziative di sicurezza;
- Promozione della cultura della sicurezza attraverso attività di comunicazione e formazione.

La politica viene periodicamente riesaminata per garantirne la coerenza con gli obiettivi aziendali e l'evoluzione normativa e tecnologica.

Saronno, 20/05/2025

La Direzione