La **CIFOLELLI EDILIZIA S.r.l.** è consapevole dell'importanza di una **POLITICA DEL SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI**) che impone, in coerenza con la missione aziendale, la gestione di tutti i processi aziendali impostata con le regole proprie dell'applicazione di tale Norma **ISO/IEC 27001 e dai controlli previsti dall'Annex A** anche in accordo con quanto già strutturato dalla **CIFOLELLI EDILIZIA S.r.l.** in conformità alle norme ISO 9001:2015 – ISO 14001:2015 – ISO 45001:2018 - ISO 37001:2016- UNI PdR 125:22- UNI 50001:2018

SCOPO-AMBITO DI APPLCIAZIONE E OBIETTIVI

La direzione di CIFOLELLI EDILIZIA S.r.l. ha definito, ha divulgato e si impegna a mantenere attiva a tutti i livelli della propria organizzazione la presente politica per la Gestione della Sicurezza delle Informazioni.

Lo scopo della presente policy è di garantire la massima soddisfazione del cliente nella fruizione dei nostri servizi e dalle nostre attività operative e la tutela e la protezione da tutte le minacce, interne o esterne, intenzionali o accidentali, delle informazioni nell'ambito delle nostre attività in accordo con le indicazioni fornite dallo standard ISO/IEC 27001 e dalle linee guida contenute nello standard ISO/IEC 27002 nelle loro ultime versioni.

AMBITO DI APPLICAZIONE

L'ambito di applicazione si rivolge a tutte le attività e servizi correlati alla Costruzione e Ristruttuazione di edifici.

OBIETTIVI -MONITORAGGIO E MIGLIORAMENTO CONTINUO

Gli obiettivi della presente politica sono:

Obiettivo 1	Proteggere in modo efficace gli asset informativi da accessi non autorizzati, modifiche non autorizzate o divulgazioni.
Tempistica	Entro dicembre 2026
Monitoraggio	Misurazione dei tempi di risposta agli incidenti, del numero di incidenti, dei risultati degli audit e della conformità agli standard.
Indicatore (KPI)	N incidenti/anno – Minimo 1 AUDIT/anno – Esecuzione di min 2 Penetration Test/anno (Devono essere eseguiti penetration test periodici nelle infrastrutture e negli applicativi per valutare la resilienza dei sistemi ad attacchi esterni ed evincere eventuali vulnerabilità e consentirne il successivo fixing)
Responsabile	RGI- Responsabile Trattamento dati

Obiettivo 2	Rispettare i requisiti normativi, contrattuali e di conformità in materia di sicurezza delle informazioni.
Tempistica	Entro dicembre 2026
Monitoraggio	Monitorare processi commerciali e di reclutamento e gestione personale come da Procedure 27001
Indicatore (KPI)	N sanzioni per non conformità in materia di sicurezza delle informazioni
Responsabile	RGI- Responsabile Trattamento dati

Obiettivo 3	Assicurare la continuità operativa dei servizi IT critici.
Tempistica	Entro dicembre 2026
Monitoraggio	Garantire adeguata manutenzione agli Asset aziendali allo scopo di evitare eventi di black out elettrici o perdita/danneggiamento dei dati
Indicatore (KPI)	N black out elettrici /anno – N di casi di perdita o danneggiamento dei dati/anno
Responsabile	RGI- Responsabile Trattamento dati

Obiettivo 4	Promuovere una cultura della sicurezza all'interno dell'organizzazione attraverso formazione e sensibilizzazione allo scopo di garantire la sicurezza dei dati, delle informazioni aziendali e dei dati personali.
Tempistica	Entro dicembre 2028
Monitoraggio	Piano di formazione annuale sulla gestione e trattamento delle informazioni al 100% del personale aziendale
Indicatore (KPI)	N % personale formato/totale personale
Responsabile	RGI- Responsabile Trattamento dati

La presente politica si applica indistintamente a tutti gli organi e i livelli dell'Azienda.
L'attuazione della presente politica è obbligatoria per tutto il personale e deve essere inserita nella regolamentazione degli accordi con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto con il trattamento di informazioni che rientrano nel campo di applicazione del Sistema di Gestione ISO 27001.
Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite attraverso i servizi forniti e localizzate in tutte le sedi dell'azienda.

È necessario assicurare:

- la riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato.
- l'integrità delle informazioni: ovvero proteggere la precisione e la completezza delle informazioni e dei metodi per la loro elaborazione.
- la disponibilità delle informazioni: ovvero che gli utenti autorizzati possano effettivamente accedere alle informazioni e ai beni collegati nel momento in cui lo richiedono.

La mancanza di adeguati livelli di sicurezza può comportare il danneggiamento dell'immagine aziendale, la mancata soddisfazione del cliente, il rischio di incorrere in sanzioni legate alla violazione delle normative vigenti nonché danni di natura economica e finanziaria.
Un adeguato livello di sicurezza è altresì basilare per la condivisione delle informazioni.
L'azienda identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che incombono sui propri asset aziendali che consente di acquisire idonea consapevolezza sul livello di esposizione a minacce.
La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate. I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.
La gestione della Sicurezza delle informazioni avviene attraverso i seguenti aspetti:

1- ASSET INVENTORY SEMPRE AGGIORNATO - Garantire un catalogo costantemente aggiornato degli asset aziendali rilevanti ai fini della gestione delle informazioni e per ciascuno deve essere individuato un responsabile. Le informazioni devono essere classificate in base al loro livello di criticità, in modo da essere gestite con livelli di riservatezza ed integrità coerenti ed appropriati.
2- VALUTAZIONE DEI RISCHI DELLE INFORMAZIONI AGGIORNATA – La valutazione dei rischi delle informazioni viene aggiornata almeno una volta all'anno in occasione del riesame della direzione o nel caso si presentino eventi avversi o nel caso vi sia un adeguamento dell'asset inventory.
3- ACCESSO AI SISTEMI SICURO - Per garantire la sicurezza delle informazioni, ogni accesso ai sistemi deve essere sottoposto a una procedura d'identificazione e autenticazione. Le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti

REVISIONE DELLA POLITICA

Questa politica è rivista almeno una volta all'anno, o ogni volta che vi sono cambiamenti significativi nell'ambiente IT o nelle normative applicabili.
Le modifiche sono approvate dalla Direzione Aziendale e comunicate a tutto il personale.

La Direzione