Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti dal **Gruppo Zeta Costruzioni Srl**, al fine di garantire un efficace e sicuro Sistema di Gestione della Sicurezza delle Informazioni.
Per il Gruppo Zeta Costruzioni Srl la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa responsabile della loro gestione. Questo significa garantire e mantenere un sistema di gestione sicuro delle informazioni, attraverso il rispetto delle seguenti proprietà:

1. ***Riservatezza:*** assicurare che l'informazione sia accessibile solamente ai soggetti e/o ai processi debitamente autorizzati;
2. ***Integrità:*** salvaguardare la consistenza dell'informazione da modifiche non autorizzate;
3. ***Disponibilità:*** assicurare che gli utenti autorizzati abbiano accesso alle informazioni e agli elementi architetturali associati quando ne fanno richiesta;
4. ***Controllo:*** assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e verificati;
5. ***Autenticità:*** garantire una provenienza affidabile dell'informazione;
6. ***Privacy:*** garantire la protezione e il controllo dei dati personali, nel rispetto della normativa vigente.

Per questo motivo il **Gruppo Zeta Costruzioni Srl ha implementato e mantiene un Sistema di Gestione della Sicurezza delle Informazioni conforme ai requisiti della Norma UNI CEI EN ISO/IEC 27001**, per garantire un'adeguata gestione della sicurezza delle informazioni nell'ambito della propria attività.
Il Sistema di Gestione della Sicurezza delle Informazioni è **certificato secondo la norma UNI CEI EN ISO/IEC 27001** ed è sottoposto a periodiche attività di verifica, monitoraggio e miglioramento.
La presente politica per la sicurezza delle informazioni si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni.
La politica della sicurezza rappresenta l'impegno dell'organizzazione nei confronti di clienti e terze parti a garantire la sicurezza delle informazioni, degli strumenti fisici, logici e organizzativi atti al trattamento delle informazioni in tutte le attività.

Obiettivo qualitativo:
Il Gruppo Zeta Costruzioni Srl definisce e persegue i seguenti obiettivi:

a) Identificare e classificare le informazioni aziendali in funzione della loro criticità e del livello di protezione necessario.
b) Prevenire accessi non autorizzati alle informazioni e garantire che il trattamento dei dati avvenga esclusivamente da parte di soggetti autorizzati.
c) Garantire che il personale e le terze parti coinvolte adottino comportamenti e procedure conformi ai requisiti di sicurezza aziendali.
d) Diffondere una cultura aziendale orientata alla sicurezza delle informazioni, attraverso attività di sensibilizzazione e formazione.
e) Rilevare, segnalare e gestire tempestivamente anomalie, incidenti e vulnerabilità che possano compromettere la sicurezza delle informazioni o la continuità delle attività aziendali.
f) Proteggere le sedi, gli uffici, i locali e le infrastrutture aziendali da accessi non autorizzati.
g) Garantire il rispetto degli obblighi normativi, contrattuali e degli impegni assunti nei confronti di clienti, fornitori e altri soggetti interessati.
h) Monitorare costantemente l'efficacia delle misure di sicurezza adottate e individuare eventuali opportunità di miglioramento.
i) Assicurare la continuità operativa e il ripristino dei sistemi e delle informazioni in caso di eventi che possano compromettere la normale operatività aziendale.

Target quantitativi:

- Mantenimento della certificazione ISO 27001;
- Audit interni annuali su 100% dei processi critici;
- Riduzione del 50% dei rischi alti entro il 2030;
- 0 incidenti critici di data breach;
- Tempo di risposta agli incidenti < 24 ore entro il 2030;

- Monitoraggio continuo degli eventi di sicurezza;
- 100% sistemi con aggiornamenti automatici entro il 2030;
- 100% dipendenti formati annualmente entro il 2030;
- Riduzione errori di pishing < 5% entro il 2030;
- Coinvolgimento dell'80% dei fornitori critici nella formazione;
- Valutazione sicurezza del 100% fornitori critici entro il 2030
- Clausole sicurezza nel 100% dei nuovi contratti entro il 2030;
- 0 sanzioni o violazioni gravi;
- 100% conformità normativa.

La Direzione è responsabile del sistema di gestione sicura delle informazioni, in coerenza con l'evoluzione del contesto aziendale e di mercato, valutando eventuali azioni da intraprendere a fronte di eventi come:

- evoluzioni significative del business;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro delle informazioni.

