Politica e controlli per la sicurezza delle informazioni

Rev.	Data	Modifiche	Redatto	Verificato	Classificazione
0	28/06/2018	Prima emissione	M.Gianordoli	M.Gianordoli	Pubblico
1	13/01/2025	Passaggio alla norma ISO/IEC 27001:2022	M.Gianordoli	M.Gianordoli	Pubblico

1. SCOPO E CAMPO DI APPLICAZIONE

Lo scopo del presente documento è quello di descrivere i principi generali di sicurezza delle informazioni definiti da Socialit al fine di sviluppare un efficiente e sicuro Sistema di Gestione della Sicurezza delle Informazioni.

2. RIFERIMENTI

- ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems - Requirements.
- Decreto legislativo 30 giugno 2003, n. 196 così come modificato dal D.Lgs. 101/2018 – Provvedimenti del Garante e Regolamento Europeo 679/2016 in materia di protezione dei dati personali.

3. DESCRIZIONE

Per Socialit la sicurezza delle informazioni ha come obiettivo primario la protezione dei dati e delle informazioni, della struttura tecnologica, fisica, logica ed organizzativa, e la loro gestione. Questo significa ottenere e mantenere un sistema di gestione sicura 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 testati;

5. **Autenticità**: garantire una provenienza affidabile dell'informazione.
6. **Privacy**: garantire la protezione ed il controllo dei dati personali

Nell'ambito della gestione dei servizi offerti, con l'osservanza dei livelli di sicurezza stabiliti, si intende assicurare:

- la garanzia di aver incaricato un partner affidabile al trattamento del proprio patrimonio informativo;
- un'elevata immagine aziendale;
- la completa osservanza delle Service Level Agreement stabilite con i clienti;
- la soddisfazione del cliente;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza

Per questo motivo Socialit ha sviluppato un sistema di gestione sicura delle informazioni seguendo i requisiti specificati della Norma ISO/IEC 27001:2022 e delle leggi cogenti come mezzo per gestire la sicurezza delle informazioni nell'ambito della propria attività.

4. AMBITO DI APPLICAZIONE

La politica per la sicurezza delle informazioni di Socialit si applica a tutto il personale interno ed alle terze parti che collaborano alla gestione delle informazioni ed a tutti i processi e risorse coinvolte nella progettazione, realizzazione, avviamento ed erogazione continuativa dei propri servizi IT.

5. DESCRIZIONE DELLA POLITICA

La politica della sicurezza di Socialit 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.

La politica della sicurezza delle informazioni di Socialit si ispira ai seguenti principi:

1. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.
2. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.
3. Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza.
4. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business.

5. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.
6. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.
7. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni.
8. Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite.

La politica della sicurezza delle informazioni viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa con l'organizzazione, le terze parti ed i clienti, attraverso un sistema documentale interno e specifici canali di comunicazione.

6. RESPONSABILITÁ ED AGGIORNAMENTI

La Direzione di Socialit 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;