1 Introduzione

1.1 Campo di applicazione

Redder Telco S.r.l.

1.2 Scopo

Questo documento descrive la politica che Redder adotta per la sicurezza delle informazioni.
Trova applicazione in ogni interazione che coinvolga dipendenti, consulenti, fornitori o terze parti.

1.3 Riferimenti

ISO 27001:2022

2 Obiettivi

2.1 **Riservatezza:** crediamo nella protezione delle informazioni, preservandole da ogni rischio di divulgazione o accesso non autorizzato.

2.2 **Integrità:** la veridicità e l'affidabilità delle informazioni è fondamentale. Questo ci permette di operare con certezza, precisione e conformità normativa.

2.3 **Disponibilità:** assicuriamo l'accesso alle informazioni in ogni momento in cui gli utenti autorizzati ne hanno bisogno.

2.4 **Conformità Legale:** il nostro operato si allinea alle leggi e normative, assicurando un rispetto totale dei requisiti contrattuali e legali.

3 Responsabilità

3.1 **Direzione:** la direzione di Redder è fortemente impegnata nella sicurezza, fornendo risorse e orientamento chiaro per assicurare una gestione efficace.

3.2 **Responsabile del sistema di gestione (RSG):** si fa carico di guidare l'elaborazione, l'implementazione, il monitoraggio e il miglioramento continuo della nostra politica. La sua collaborazione con ogni reparto assicura misure di sicurezza efficaci.

3.3 **Dipendenti:** hanno l'obbligo di comprendere e seguire le nostre regole sulla sicurezza delle informazioni. Ogni potenziale violazione viene comunicata al proprio responsabile o all'RSG e viene gestita con serietà e dedizione.

4 Classificazione delle informazioni

Le informazioni sono valutate e classificate riflettendo il loro valore e sensibilità. Questo permette di applicare misure di sicurezza mirate.

5 Gestione degli accessi

Gli accessi alle informazioni vengono determinati dal ruolo e dalla necessità della persona che tratta l'informazione. I privilegi vengono modificati prontamente al variare dei presupposti sul quale è stato rilasciato l'accesso. L'autenticazione degli utenti è basata su credenziali uniche e segrete, gestite attraverso sistemi di password management, anche con metodi di autenticazione a doppio fattore, chiavi e certificati.

6 Gestione dei dispositivi e delle reti

I dispositivi aziendali sono protetti con soluzioni di sicurezza aggiornate e con uno stack di sicurezza moderno quali firewall, EDR, IDS/IPS, SIEM e patch management. Le reti sono segmentate.

7 Gestione dei rischi e degli incidenti

Vengono identificate proattivamente minacce e vulnerabilità, mettendo in atto strategie documentate attraverso un processo di analisi del rischio volto a mitigare ogni potenziale minaccia. Gli eventi di sicurezza vengono gestiti in modo rapido ed efficace attraverso il piano di risposta agli incidenti.

8 Consapevolezza della sicurezza

Attraverso programmi di formazione e sensibilizzazione regolari, viene mantenuta alta l'attenzione e l'impegno di tutti.

9 Conformità e revisione

Vengono effettuati audit interni regolari e revisioni periodiche permettendo di adeguare la politica a nuove minacce, tecnologie e normative. Vengono prese azioni disciplinari nei confronti di chi non applica la presente politica.

10 Miglioramento continuo

Vengono continuamente affinate le nostre tattiche e i metodi per rispondere all'evoluzione delle minacce e dei rischi che si presentano. Questa politica e i documenti ad essa collegati saranno sottoposti a revisione periodica e tutte le parti coinvolte ne saranno notificate.