PREX®	**Politica della Sicurezza delle Informazioni**	**DOC002 – Ver. 1.0** del 10-05-2023 Autore: RSGSI Approvato da: Direzione Tipo Documento: Pubblico

La sicurezza e la salvaguardia del patrimonio informativo costituiscono condizione imprescindibile per il raggiungimento degli obiettivi di business di PREX srl.

I requisiti per la sicurezza delle informazioni sono coerenti con gli obiettivi aziendali e il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) rappresenta lo strumento che consente la condivisione delle informazioni, lo svolgimento di operazioni corrette e la riduzione dei rischi connessi alle informazioni a livelli accettabili.

In considerazione di ciò, lo svolgimento delle attività aziendali deve sempre avvenire garantendo adeguati livelli di riservatezza, integrità e disponibilità delle informazioni attraverso l'adozione di un formale "*Sistema di Gestione della Sicurezza delle Informazioni*" (SGSI) in linea con i requisiti attesi dagli stakeholder di PREX srl e nel rispetto delle normative vigenti, come qui definite:

1. **Riservatezza:** proprietà per cui l'informazione non è resa disponibile o rivelata a individui, entità o processi non autorizzati;
2. **Integrità**: proprietà relativa alla salvaguardia dell'accuratezza e della completezza delle informazioni e dei beni ad esse collegati;
3. **Disponibilità**: proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata;

In particolare, il Sistema di Gestione della Sicurezza delle Informazioni è applicato alla:

Gestione della sicurezza dei dati inerenti la progettazione, sviluppo, manutenzione ed assistenza di software in ambito medico-formativo, digital health, erogato on premise o in modalità cloud SaaS.

Gli obiettivi generali del SGSI perseguiti con l'impegno della direzione, sono:

- dimostrare agli stakeholders la propria capacità di fornire con regolarità servizi informatici sicuri, massimizzando gli obiettivi di sicurezza;
- minimizzare il rischio di perdita e/o indisponibilità dei dati gestiti, pianificando e gestendo le attività a garanzia della continuità di servizio;
- svolgere una continua e adeguata analisi dei rischi che esamini costantemente le vulnerabilità e le minacce associate alle attività a cui si applica il sistema;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere;
- promuovere la collaborazione, comprensione e consapevolezza del SGSI da parte dei fornitori strategici;
- conformarsi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti che disciplinano le attività in cui opera l'azienda, tra i quali, in particolare le regolamentazioni inerenti ai trattamenti dei dati personali e la loro sicurezza (GDPR e normative nazionali).

Tutto il personale, nell'ambito delle relative responsabilità, è coinvolto nella segnalazione al Responsabile del Sistema di Gestione della Sicurezza delle Informazioni (RSGSI) di eventuali eventi negativi o incidenti riscontrati e di qualsiasi debolezza identificata nel SGSI.

Tutta l'organizzazione, a partire dai vertici, è impegnata a supportare l'implementazione, la messa in opera e il riesame periodico per il miglioramento continuo del SGSI.

Il vertice aziendale si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi di questa politica.