MEDISOLVE
HEALTH TECH SOLUTIONS

INFORMATION SECURITY POLICY

CODE	REV	DATE	CLASSIFICATION
PL.SGI.01	00	30/03/2026	PUBLIC

1. Premessa

1.1 Matrice della redazione e delle revisioni

REVISION	DESCRIPTION	EDITING		VERIFICATION		APPROVAL	
		Date	**Name Signature**	**Date**	**Name Signature**	**Date**	**Name Signature**
00	First issue Medisolve Group	26/01/2026	Nicolas Fiorio 	27/01/2026	Noemi Alloa Casale 	30/03/2026	Approved by CDA

2. La politica

La Direzione del gruppo Medisolve (nel seguito "Gruppo") riconosce che le informazioni rappresentano un patrimonio strategico per l'organizzazione e si impegna a proteggerle da minacce interne ed esterne, intenzionali o accidentali.

Il Gruppo istituisce, mantiene e migliora continuamente un Sistema di Gestione Integrato (SGI) che include anche la Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001:2022, adottando un approccio basato sull'analisi e sul trattamento dei rischi per la sicurezza delle informazioni.

Il SGSI si applica a tutte le informazioni trattate dal Gruppo, indipendentemente dal formato o dal supporto, ed è finalizzato a garantire in modo sistematico:

- riservatezza, assicurando che le informazioni siano accessibili esclusivamente a soggetti autorizzati;
- integrità, tutelando l'accuratezza e la completezza delle informazioni e dei processi di trattamento;
- disponibilità, garantendo che le informazioni e i servizi siano accessibili quando richiesto.

Nella definizione e nell'attuazione del SGSI, il Gruppo tiene conto:

- del contesto interno ed esterno e delle esigenze delle parti interessate;
- dei requisiti legali, normativi, regolamentari e contrattuali applicabili;
- degli obiettivi strategici e delle esigenze di continuità operativa.

Il Gruppo assicura che i rischi per la Sicurezza delle Informazioni siano valutati periodicamente e trattati in modo proporzionato, tenendo conto del rischio d'impresa, della sostenibilità economica e delle migliori pratiche di settore.

I principi fondamentali che guidano la gestione della Sicurezza delle Informazioni includono:

- l'applicazione del principio del *need-to-know* e della segregazione dei ruoli;
- la protezione delle informazioni lungo tutto il loro ciclo di vita;
- la consapevolezza e la formazione continua del personale;
- la gestione dei fornitori e dei partner in relazione ai rischi di sicurezza;
- l'integrazione dei requisiti di sicurezza sin dalle fasi di progettazione dei processi e dei servizi (*security by design*).

La Direzione ha la responsabilità ultima della Sicurezza delle Informazioni, definendo gli obiettivi strategici, assegnando ruoli e responsabilità, garantendo le risorse necessarie e promuovendo una cultura aziendale orientata alla sicurezza delle informazioni.

La presente Politica è comunicata a tutto il personale e resa disponibile alle parti interessate pertinenti e riesaminata periodicamente per garantirne la continua adeguatezza, efficacia e conformità agli standard ISO/IEC 27001:2022.

English version

The Management of the Medisolve Group (hereinafter the "Group") acknowledges that information represents a strategic asset for the organization and is committed to protecting it from internal and external threats, whether intentional or accidental.

The Group establishes, maintains, and continuously improves an Integrated Management System (IMS), which also includes an Information Security Management System (ISMS) in compliance with ISO/IEC 27001:2022, adopting a risk-based approach to information security risk assessment and treatment.

The ISMS applies to all information processed by the Group, regardless of its format or medium, and is aimed at systematically ensuring:

- Confidentiality, by ensuring that information is accessible only to authorized individuals;
- Integrity, by safeguarding the accuracy and completeness of information and processing activities;
- Availability, by ensuring that information and services are accessible when required.

In defining and implementing the ISMS, the Group considers:

- the internal and external context and the needs of interested parties;
- applicable legal, statutory, regulatory, and contractual requirements;
- strategic objectives and business continuity needs.

The Group ensures that Information Security risks are periodically assessed and addressed in a proportionate manner, taking into account enterprise risk, economic sustainability, and industry best practices.

The fundamental principles guiding Information Security management include:

- application of the need-to-know principle and segregation of duties;
- protection of information throughout its entire lifecycle;
- continuous awareness and training of personnel;
- management of suppliers and partners in relation to security risks;
- integration of security requirements from the early stages of process and service design (security by design).

Management holds ultimate responsibility for Information Security by defining strategic objectives, assigning roles and responsibilities, ensuring the necessary resources, and promoting a corporate culture oriented toward information security.

This Policy is communicated to all personnel, made available to relevant interested parties, and periodically reviewed to ensure its continued suitability, effectiveness, and compliance with ISO/IEC 27001:2022.