

Politica del sistema di gestione della sicurezza delle informazioni

Documento:	PL.SGSI.01 - Politica del sistema di gestione della sicurezza delle informazioni		
Revisione:	00	Data revisione:	03/05/2023

Redazione:	Verifica:	Approvazione:
M. Barbieri	E.Setti	A.Ardesi

Riepilogo delle revisioni

Revisione	Motivo	Data
00	Prima emissione	03/05/2023

Codice doc.	Rev.	Emissione Originaria	Emissione Corrente	Classificazione
PL.SGSI.01	00	03/05/2023	03/05/2023	PUBBLICO

Dichiarazione della politica

Polygon S.p.A. offre servizi di assistenza e manutenzione di infrastrutture tecnologiche ICT a supporto dell'erogazione di teleservizi in ambito sanitario, socio-sanitario e sociale, per realtà pubbliche e private.

Trattiamo quindi dati pubblici e riservati, dati anonimi, personali comuni e/o particolari ex art. 9 del Regolamento UE 2016/679 (GDPR).

È fondamentale che sia garantita la massima sicurezza dei dati, in qualunque formato, garantendone la salvaguardia della loro riservatezza, integrità e disponibilità.

L'approccio della sicurezza dell'informazione è basato sul rischio, conformemente alla norma ISO 27001:2022 e alle migliori pratiche.

Le procedure del Sistema di Gestione della Sicurezza delle Informazioni stabiliscono i criteri di valutazione del rischio allineati con le attuali procedure e politiche di gestione del rischio strategico aziendale.

Nella valutazione dei rischi per la sicurezza delle informazioni Polygon S.p.A. tiene in debita considerazione i fattori esterni ed interni pertinenti alle sue finalità e che influenzano la sua capacità di conseguire gli esiti previsti per il proprio Sistema di Gestione della Sicurezza delle Informazioni.

Il Sistema di Gestione della Sicurezza tiene conto dei requisiti commerciali, giuridici o regolamentari e degli obblighi contrattuali in materia di sicurezza delle informazioni, cybersecurity e protezione dei dati personali.

Devono essere sempre garantiti livelli di sicurezza che assicurino il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione del rischio, politiche e strategie aziendali, politiche e strategie dei fornitori e dei clienti, necessità di costante adeguamento al contesto in cui operiamo e di miglioramento dell'efficacia ed efficienza dei processi e controlli di sicurezza.

I principi cardine a cui attenersi sono:

- le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio need to know) e nei tempi, e nelle modalità stabiliti;
- le informazioni devono essere protette al fine di garantirne la riservatezza, la disponibilità e l'integrità;
- il personale deve essere opportunamente formato in materia di sicurezza delle informazioni; e deve seguire i principi etici e comportamentali prescritti;
- i fornitori devono essere opportunamente tenuti sotto controllo attraverso misure stabilite adeguate al contesto;
- i partner devono essere selezionati anche per la loro capacità e disponibilità a conformarsi alle nostre regole di sicurezza;
- per i servizi erogati, è necessario considerare i requisiti di sicurezza sin dalla fase di progettazione;

La responsabilità finale della sicurezza delle informazioni ricade sulla Direzione che può delegare attività ai responsabili delle aree organizzative aziendali.

La Direzione ha il compito di istituire e migliorare continuamente il Sistema di Gestione della Sicurezza fornendo il quadro per la definizione degli obiettivi, stabilendo un senso complessivo di indirizzo dei principi di azione in materia di sicurezza.

Questa politica è comunicata a tutto il personale attraverso la pubblicazione nella intranet aziendale e alle parti interessate attraverso la pubblicazione sul sito web istituzionale.

Il presente documento sostituisce ogni altra eventuale versione precedente ed è in vigore dal 08/05/2023; viene periodicamente riesaminato e comunque con cadenza almeno annuale al fine di garantire il rispetto dei requisiti della norma ISO 27001:2022

Codice doc.	Rev.	Emissione Originaria	Emissione Corrente	Classificazione
PL.SGSI.01	00	03/05/2023	03/05/2023	PUBBLICO