POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

SISTEMA DI GESTIONE DELLA SICUREZZA DELLE INFORMAZIONI (SGSI)
ISO/IEC 27001:2022

INFORMAZIONI DOCUMENTO

Codice	Pol000-SGSI
Titolo	Politica per la Sicurezza delle Informazioni (SGSI)
Versione	1
Data Emissione	16 maggio 2026
Classificazione	L2 - PROTETTO
Titolare	RSGSI - Mariagrazia Silvestro
Data Protection Officer	Giuditta Russo
Approvazione	Amministratore Unico - Michele Laranga

1. Impegno della Direzione

La Direzione di Tecnolife SRL, è consapevole del valore strategico delle informazioni per l'attività di progettazione, sviluppo e commercializzazione di software, dispositivi medici, apparecchiature elettromedicali e di laboratorio e ogni alto dispositivo e presidio ad uso sanitario. Pertanto si impegna a stabilire, attuare, mantenere e migliorare continuamente un Sistema di Gestione della Sicurezza delle Informazioni (SGSI) conforme alla norma ISO/IEC 27001:2022.

La Direzione:

- si assume la responsabilità dell'efficacia del SGSI; promuove una cultura della sicurezza e della protezione dei dati a tutti i livelli dell'organizzazione.
- Assicura le risorse umane, tecniche e finanziarie necessarie all'implementazione e al miglioramento dei controlli di sicurezza definiti nelle policies aziendali e nello Statement of Applicability (SOA).
- Approva e riesamina: questa Politica, le policies del Documentazione e il SOA sono approvati dall'Amministratore Unico e riesaminati almeno annualmente.

- La Politica è comunicata a tutto il personale in ingresso e ad ogni aggiornamento di ruolo, la stessa è resa disponibile alle parti interessate esterne su richiesta, è pubblicata nel sito Web aziendale www.tecnolifesrl.it.

2. Obiettivi della Sicurezza delle Informazioni

- Proteggere la riservatezza, l'integrità e la disponibilità delle informazioni aziendali, dei clienti, degli utenti, dei fornitori, dei partner, in ogni forma e supporto.
- Garantire la continuità operativa dei servizi critici (piattaforma web, gestionale, sviluppo software, assistenza tecnica) secondo gli obiettivi di ripristino definiti nella Business Impact Analysis.
- Assicurare la conformità ai requisiti legali, regolamentari e contrattuali applicabili, in primo luogo GDPR 2016/679, Reg. (UE) 2024/1689 (AI Act), la normativa sui dispositivi medici e gli accordi con clienti e fornitori.
- Prevenire, rilevare e rispondere agli incidenti di sicurezza, con apprendimento sistematico dagli eventi.
- Gestire i rischi per la sicurezza delle informazioni con un approccio basato sul rischio, proporzionato al contesto e agli impatti per l'organizzazione e per gli interessati.
- Presidiare l'uso responsabile dei sistemi di intelligenza artificiale, in coerenza con l'AI Act e con le policies aziendali sull'uso responsabile dell'IA.
- Migliorare continuamente il SGSI sulla base di audit, indicatori, incidenti e riesami di direzione.

3. Ambito di Applicazione

Questa Politica si applica a tutte le sedi, ai sistemi informativi, alle reti digitali, alle apparecchiature, ai dati ed informazioni di Tecnolife SRL, nonché a tutto il personale (dipendenti e collaboratori), ai fornitori e ai terzi che accedono o trattano risorse informative dell'azienda, in qualunque ubicazione (sede, smart working, mobilità) e su qualunque dispositivo (aziendale o autorizzato).

- Il perimetro comprende i dati personali trattati, il codice sorgente proprietario, le informazioni dei clienti e degli utenti, le credenziali di accesso e ogni altra informazione classificata secondo le politiche aziendali.
- L'accesso ai sistemi e ai dati aziendali implica l'accettazione di questa Politica e delle policies del Documentazione.

4. Principi Fondamentali

I controlli implementati da Tecnolife SRL si basano sui seguenti fattori:

- **Approccio basato sul rischio:** i controlli sono selezionati, implementati e verificati in relazione ai rischi valutati e agli impatti per l'organizzazione e per gli interessati.
- **Conformità:** il rispetto di leggi, normative, contratti e policy è obbligatorio per tutti; la conformità è monitorata e verificata.
- **Minimo privilegio e need-to-know:** accessi e diritti sono limitati al necessario per ruolo e finalità.

- **Classificazione delle informazioni:** ogni informazione è classificata ed etichettata secondo le policies aziendali.
- **Protezione fin dalla progettazione e by default:** sicurezza e privacy sono integrate in progetti, sviluppo software e processi (Art. 25 GDPR).
- **Separazione dei compiti:** compiti in conflitto sono separati; le eccezioni sono documentate e approvate.
- **Ciclo di vita sicuro degli asset e degli accessi:** gestione autorizzata dall'assegnazione (screening, consegna asset, cyber igiene) allo screening di uscita, revoca e restituzione.
- **Continuità e ripristino:** backup, ridondanze, piani di emergenza ed esercitazioni garantiscono la continuità secondo gli obiettivi della BIA.
- **Uso responsabile dell'IA:** strumenti di IA solo se autorizzati, senza dati riservati in tool non approvati, con verifica umana degli output e contromisure anti-phishing/deepfake (sezione AI di ciascuna policy).
- **Miglioramento continuo:** audit, analisi post-incidente, indicatori e riesami alimentano il miglioramento del SGSI.

5. Ruoli e Responsabilità

La governance della sicurezza e della privacy è assegnata a ruoli definiti e documentati:

Ruolo	Responsabilità principali
Amministratore Unico (Michele Laranga)	Approvazione di politica, SOA, budget e obiettivi; massima responsabilità del SGSI
RSGSI (Mariagrazia Silvestro)	Presidio del SGSI, gestione dei rischi, coordinamento incidenti e audit
DPO (Giuditta Russo)	Conformità GDPR, DPIA, rapporti con il Garante, diritti degli interessati
Team IT	Implementazione e operatività dei controlli tecnici: accessi, reti, backup, logging, monitoraggio
Responsabili di funzione	Applicazione delle policies nei propri ambiti, gestione accessi del personale
Tutti i dipendenti e collaboratori	Rispetto di questa Politica e del Documentazione, formazione obbligatoria, dovere di segnalazione

6. Documentazione del SGSI

Questa Politica è il documento capostipite del SGSI ed è attuata dal seguente Documentazione, approvato e versionato:

- Statement of Applicability con la mappatura completa dei 93 controlli dell'Annex A di ISO/IEC 27001:2022.
- Le policies aziendali che garantiscono: governance, gestione asset, uso accettabile delle risorse, accessi, fornitori, incidenti, continuità, compliance, revisione, smart working, clear desk, sicurezza operativa, backup, log, monitoraggio, software, rete, filtri web, crittografia, outsourcing, sviluppo sicuro ed end-point, post-incidenti e prove, cessazione e rapporto di lavoro, sicurezza fisica.
- Documenti operativi: moduli, Mansionario dei Ruoli, Piani Formativi e Registrazioni Incontri Formativi, modulo di autorizzazione al trattamento dei dati ex Art. 29 GDPR, Business Impact Analysis BIA, ecc.
- Evidenze operative: file di configurazione degli asset e degli amministratori autorizzati, matric degli accessi, report di back-up, archivio log-firewall, registro prove UPS, registro cambio password, report di penetration test, ecc.

7. Gestione del Rischio e dei Controlli

- La valutazione dei rischi per la sicurezza delle informazioni è condotta almeno annualmente e alla verifica di risultati di audit, incidenti rilevanti o cambiamenti significativi.
- I controlli di sicurezza sono selezionati dall'Annex A di ISO/IEC 27001:2022 e documentati nel SOA; le esclusioni sono giustificate.
- L'efficacia dei controlli è misurata tramite indicatori, audit interni ed esterni, test di ripristino e penetration test periodici.

8. Conformità Legale, Regolamentare e Contrattuale

- GDPR 2016/679: principi di protezione dei dati, DPIA ove necessaria, gestione dei diritti degli interessati, notifica delle violazioni entro 72 ore (Artt. 33-34).
- Reg. (UE) 2024/1689 (AI Act): uso responsabile e trasparente dei sistemi di IA.
- Normativa sui dispositivi medici e sulla documentazione tecnica applicabile ai prodotti Tecnolife, con riferimento alla sicurezza dei dati dei pazienti e delle prestazioni.
- Requisiti contrattuali con clienti, fornitori e partner, incluse clausole di sicurezza e notifica incidenti.
- Normativa del lavoro e CCNL applicabili per screening, obblighi del personale e procedimenti disciplinari.

9. Formazione e Sensibilizzazione

- Il personale riceve formazione obbligatoria all'ingresso e con cadenza almeno annuale (GDPR/privacy, cybersecurity operativa con anti-phishing e deepfake, NIS2 e gestione incidenti, AI Act).

- La formazione è tracciata nei Registri Incontri Formativi e tenuta sotto controllo dal RSGSI.
- Campagne periodiche di phishing simulation e comunicazioni di sensibilizzazione completano il programma.

10. Violazioni e Sanzioni

- Le violazioni di questa Politica e del Documentazione sono gestite secondo la gestione degli incidenti, il processo disciplinare e le conseguenze contrattuali e legali previste.
- Ogni violazione, sospetta o accertata, deve essere segnalata tempestivamente; la mancata segnalazione è a sua volta violazione.
- I fornitori e i collaboratori esterni sono soggetti alle sanzioni e alle risoluzioni contrattuali previste dagli accordi vigenti.

11. Revisione della Politica

Questa Politica è riesaminata almeno annualmente dall'Amministratore Unico, su proposta del RSGSI, e comunque dopo incidenti rilevanti, audit significativi o cambiamenti che impattano sulla sicurezza delle informazioni.

DICHIARAZIONE DI APPROVAZIONE

Il sottoscritto Amministratore Unico di Tecnolife SRL approva la presente Politica per la Sicurezza delle Informazioni (SGSI), impegnando l'organizzazione alla sua attuazione e al miglioramento continuo del Sistema di Gestione della Sicurezza delle Informazioni conforme a ISO/IEC 27001:2022.

Data: 16/05/2026

Michele Laranga

Amministratore Unico
Tecnolife SRL