Pubblico

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	09/02/2026	Elena Ciampi	Stefano Linari

Indice

Scopo

La presente politica esprime l'impegno del Top Management di Linari Medical S.r.l. verso la protezione sistematica degli asset informativi dell'organizzazione. In quanto documento quadro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), essa definisce il riferimento strategico per istituire, attuare, mantenere e migliorare continuamente le misure di sicurezza che tutelano la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito della commercializzazione di dispositivi medici di classe I e dell'erogazione dei servizi tramite la piattaforma cloud.

L'organizzazione riconosce che la fiducia di ospedali pubblici, clinici, pazienti e autorità regolatorie dipende dalla capacità di proteggere le informazioni lungo l'intero ciclo di vita — dalla raccolta alla dismissione — e intende garantire tale protezione attraverso un approccio basato sul rischio, il rispetto dei requisiti normativi applicabili e il coinvolgimento di tutto il personale nella cultura della sicurezza.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi, i sistemi tecnologici e la sede operativa di Linari Medical S.r.l. situata in Via Gaetano Malasoma 26, 56121 Pisa (PI). Coinvolge tutto il personale interno, i collaboratori a contratto, i fornitori critici — inclusi Linari Engineering per la fabbricazione dei dispositivi, i contractor esterni per lo sviluppo software e il fornitore di servizi cloud — e qualunque terza parte che acceda alle informazioni o ai sistemi aziendali.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Riservatezza** : proprietà per cui l'informazione non è resa disponibile o divulgata a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.
- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi.

- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa a un sistema, un servizio o una rete che indica una possibile violazione della politica di sicurezza, un guasto dei controlli o una situazione non nota in precedenza che può avere rilevanza per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni, indesiderati o imprevisti, che hanno una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Asset** : qualsiasi elemento che ha valore per l'organizzazione, incluse informazioni, software, hardware, servizi, persone, e la relativa reputazione.
- **Controllo** : misura che modifica il rischio.

Ruoli e responsabilità

- **CEO** : approva la presente politica e ne assicura l'adeguatezza rispetto agli obiettivi strategici dell'organizzazione.
- **CTO & Chairman** : promuove l'allocazione delle risorse necessarie al SGSI e supervisiona l'integrazione della sicurezza delle informazioni nella strategia tecnologica e di prodotto.
- **CIO / CISO** : coordina l'attuazione, il monitoraggio e il miglioramento continuo del SGSI, curandone la comunicazione a tutto il personale e alle parti interessate.
- **Management System Manager** : supporta la conformità documentale del SGSI e ne integra i requisiti con il sistema di gestione per la qualità.
- **HR** : garantisce che i requisiti di sicurezza delle informazioni siano inclusi nei processi di selezione, formazione e cessazione del rapporto di lavoro.
- **Tutto il personale e le terze parti autorizzate** : rispettano la presente politica e le politiche di dettaglio, segnalando tempestivamente eventi di sicurezza osservati o sospetti.

Obiettivi di sicurezza delle informazioni

Linari Medical S.r.l. persegue obiettivi di sicurezza delle informazioni coerenti con il proprio contesto organizzativo, la valutazione dei rischi e gli indirizzi emersi dal riesame della direzione. Gli obiettivi sono definiti in modo misurabile, corredati da indicatori, risorse, responsabilità e scadenze temporali, e vengono registrati nel programma di miglioramento sottoposto al riesame periodico del **CTO & Chairman** .

In particolare, l'organizzazione si impegna a:

- preservare la riservatezza delle informazioni dei pazienti, dei dati di progettazione dei dispositivi medici e delle informazioni commerciali strategiche, assicurando che l'accesso sia concesso esclusivamente in base al principio della necessità di conoscenza;

- garantire l'integrità dei dati gestiti dalla piattaforma Linari Medical Cloud e dai sistemi informativi aziendali, prevenendo modifiche non autorizzate e mantenendo la tracciabilità delle operazioni;
- assicurare la disponibilità dei servizi e dei sistemi critici, definendo livelli di servizio adeguati alle esigenze degli ospedali pubblici clienti e pianificando la continuità operativa;
- mantenere la conformità ai requisiti regolatori applicabili, con particolare attenzione agli obblighi verso l'Agenzia per la Cybersicurezza Nazionale (ACN);
- promuovere una cultura della sicurezza attraverso programmi di sensibilizzazione e formazione rivolti a tutto il personale.

Il **CIO / CISO** raccoglie periodicamente i dati di monitoraggio, li confronta con i target pianificati e presenta una sintesi al riesame della direzione, che delibera sulla chiusura, l'estensione o la revisione di ciascun obiettivo.

Principi fondamentali di sicurezza delle informazioni

Linari Medical S.r.l. fonda il proprio SGSI su un insieme di principi che guidano tutte le politiche di dettaglio, le procedure operative e le decisioni quotidiane in materia di sicurezza.

Approccio basato sul rischio. L'organizzazione adotta una metodologia strutturata di valutazione del rischio che utilizza una matrice probabilità-impatto su scala 1–4 e classifica i rischi in tre livelli — basso (1–5), medio (6–9) e alto (10–16). Ogni rischio pari o superiore alla soglia di tolleranza è soggetto a un piano di trattamento che può prevedere mitigazione, trasferimento, eliminazione o accettazione informata, con approvazione proporzionata al livello di rischio. Tale valutazione informa la selezione dei controlli e viene riesaminata almeno annualmente o in occasione di cambiamenti significativi.

Responsabilità condivisa. La sicurezza delle informazioni non è delegata a un'unica funzione: ogni persona che accede agli asset informativi dell'organizzazione è responsabile della loro protezione. L'organigramma di sicurezza attribuisce responsabilità specifiche dal Top Management fino ai singoli collaboratori, come formalizzato nella *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* .

Uso accettabile delle risorse. L'organizzazione stabilisce regole chiare per l'utilizzo delle informazioni e degli asset associati, proporzionate al livello di classificazione assegnato a ciascun dato. Tali regole comprendono le modalità autorizzate di accesso, trasmissione e conservazione, nonché i divieti volti a prevenire compromissioni derivanti da uso improprio. I principi operativi sono dettagliati nella *POL Politica di sicurezza operativa* e nella *POL Politica di classificazione ed etichettatura delle informazioni* .

Protezione dello schermo e dell'area di lavoro. Considerato che l'organizzazione opera in ambienti di coworking condivisi, ogni dispositivo aziendale adotta il blocco automatico dello schermo dopo un periodo di inattività e richiede l'autenticazione al ripristino. L'area di lavoro è allestita in modo da impedire la visione dello schermo a persone non autorizzate, e i documenti riservati non sono mai lasciati visibili su scrivanie o stampanti.

Segnalazione tempestiva degli eventi di sicurezza. L'organizzazione promuove una cultura nella quale ogni collaboratore segnala immediatamente, attraverso i canali stabiliti,

qualunque evento di sicurezza osservato o sospetto — comprese violazioni delle politiche, anomalie nei sistemi e potenziali vulnerabilità — senza timore di conseguenze negative. Il meccanismo di segnalazione e la successiva gestione degli eventi sono formalizzati nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Classificazione e trattamento proporzionale. Le informazioni sono classificate in base alla loro sensibilità e trattate con controlli proporzionati al livello di criticità, secondo il framework documentato nella *POL Politica di classificazione ed etichettatura delle informazioni* .

Miglioramento continuo. Il SGSI è sottoposto a un ciclo costante di verifica e perfezionamento alimentato da audit interni, analisi degli incidenti, risultati del monitoraggio degli indicatori e feedback delle parti interessate. I risultati confluiscono nel riesame della direzione, che definisce gli indirizzi per l'evoluzione del sistema.

Conformità normativa e contrattuale. L'organizzazione si impegna a soddisfare i requisiti legali, regolamentari e contrattuali applicabili alla sicurezza delle informazioni, con particolare attenzione agli obblighi nei confronti di ACN per l'accreditamento come fornitore di ospedali pubblici.

Protezione degli asset fuori sede

Linari Medical S.r.l. si impegna a garantire che gli asset informativi mantengano un livello di protezione adeguato anche quando si trovano al di fuori della sede aziendale. Poiché l'organizzazione non prevede modalità di lavoro da remoto, gli scenari fuori sede riguardano esclusivamente trasferte di personale, consegne a fornitori o consulenti e trasporto di supporti fisici per esigenze operative o di rappresentanza.

Sono considerati asset fuori sede, a titolo indicativo: notebook e dispositivi mobili utilizzati durante trasferte commerciali o tecniche, supporti fisici contenenti dati aziendali e documenti cartacei trasportati per esigenze di rappresentanza o dimostrazione presso strutture sanitarie clienti.

L'organizzazione adotta i seguenti principi di protezione:

- **Custodia** : gli asset non sono mai lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di hotel o spazi di coworking esterni. In trasferta il personale assegnatario li custodisce in luogo chiuso a chiave o nella cassaforte della struttura ospitante.
- **Trasporto** : l'asset rimane sotto la custodia personale del collaboratore incaricato. Il trasporto in stiva di bagaglio aereo e l'invio mediante posta ordinaria non sono ammessi; le consegne a fornitori o sedi terze avvengono tramite corriere tracciato.
- **Segnalazione di smarrimento, furto o danneggiamento** : il personale notifica immediatamente al **CIO / CISO** — e comunque entro ventiquattro ore dall'accadimento — qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le misure di blocco remoto del dispositivo, revoca degli accessi e sostituzione delle credenziali, e l'evento è registrato come incidente di sicurezza delle informazioni nel *MOD Registro degli incidenti di sicurezza delle informazioni* .
- **Restituzione** : al termine della trasferta o del rapporto di collaborazione, l'asset è restituito all'organizzazione secondo le modalità definite nella *PRO Procedura di configurazione, gestione e smaltimento degli asset* .

Archiviazione e aggiornamento

La presente politica è un documento controllato, archiviato nel sistema di gestione documentale aziendale e accessibile a tutto il personale autorizzato. Il **CIO / CISO** ne cura il riesame almeno annuale, oppure in occasione di cambiamenti significativi nell'organizzazione, nella tecnologia, nel panorama delle minacce o nel quadro normativo applicabile. Ogni revisione richiede l'approvazione del **CEO** e la successiva comunicazione a tutte le parti interessate; le versioni superate sono conservate a fini di audit e contrassegnate come obsolete.

Documenti di riferimento

- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione dei rischi