POLITICA DI SICUREZZA DELLE INFORMAZIONI

Codice documento:	**POL-400_GRP_IT v08**
Funzione approvante:	**Consiglio di Amministrazione Lutech S.p.a.**
Data approvazione:	**06/08/2026**

CLASSIFICAZIONE

Pubblico

SOMMARIO MODIFICHE

Ver.	Data	Descrizione Modifiche
01	03/04/2018	Prima emissione (POL-SGSI).
02	02/05/2019	Rinominata in MSI-POL, rivisti i contenuti.
03	22/10/2020	Revisione generale nei contenuti e forma; inseriti riferimenti puntuali su norme ISO.
04	20/05/2022	Aggiornati obiettivi.
05	11/03/2024	Modificata versione norma 27001:2022.
06	25/05/2024	Aggiornata definizione PII con dati personali invece di informazioni personali identificabili.
07	27/03/2026	Revisione generale della MSI-POL contenuti e forma; adozione template standard.
08	06/08/2026	Revisione generale per NIS2

INDICE

1 INTRODUZIONE

Il patrimonio informativo del Gruppo Lutech costituisce un asset strategico essenziale per il perseguimento degli obiettivi aziendali, l'erogazione dei servizi, l'innovazione, la tutela del know-how e la creazione di valore per clienti, partner e altre parti interessate. In quanto asset strategico, esso deve essere adeguatamente protetto attraverso un costante bilanciamento tra il livello di rischio accettato e il livello di protezione richiesto, coniugando la tutela delle informazioni con l'efficienza, l'efficacia e la continuità dei processi aziendali.

In un contesto caratterizzato dalla crescente digitalizzazione, dall'evoluzione delle minacce informatiche e dal coinvolgimento di un numero sempre maggiore di stakeholder, la sicurezza delle informazioni rappresenta un elemento fondamentale per garantire la resilienza dell'Organizzazione, la tutela del patrimonio informativo, la continuità dei servizi e il mantenimento della fiducia di clienti, partner e altre parti interessate.

2 SCOPO

La presente Politica definisce i principi e gli impegni adottati dal Gruppo Lutech per garantire la protezione delle informazioni e degli asset informativi trattate nell'ambito delle proprie attività.

Essa stabilisce il quadro di riferimento per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni, nel rispetto delle disposizioni legislative, regolamentari e contrattuali contribuendo alla continuità operativa e alla tutela degli interessi aziendali e dei clienti.

La presente Politica costituisce inoltre il riferimento per la definizione e l'attuazione delle misure organizzative, procedurali e tecniche adottate dalle Società del Gruppo in materia di sicurezza delle informazioni.

3 AMBITO DI APPLICAZIONE

La presente Politica si applica a tutte le Società del Gruppo Lutech e a tutto il personale, inclusi collaboratori, consulenti, fornitori, partner e altre terze parti che, a qualsiasi titolo, trattano informazioni o accedono agli asset informativi del Gruppo.

La Politica si applica a tutti i processi, ai prodotti, ai servizi e agli asset informativi gestiti dalle Società del Gruppo e riguarda tutte le informazioni trattate, indipendentemente dal formato, dal supporto o dalla tecnologia utilizzata.

4 RIFERIMENTI NORMATIVI

- **ISO/IEC 27001:2022** - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO/IEC 27002:2022** - Information security, cybersecurity and privacy protection — Information security controls
- **ISO/IEC 27005:2022** - Information security, cybersecurity and privacy protection — Guidance on managing information security risks
- **ISO/IEC 27017:2015** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- **ISO/IEC 27018:2025** - Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors
- **Direttiva (UE) 2022/2555 (NIS2**), ove applicabile;
- **Regolamento (UE) 2016/679 (GDPR),** ove applicabile;

La presente Politica è adottata nel rispetto delle disposizioni legislative, regolamentari e contrattuali applicabili nei Paesi in cui operano le Società del Gruppo e costituisce il riferimento comune per la definizione e l'attuazione delle misure di sicurezza delle informazioni.
Le Società del Gruppo assicurano il rispetto degli eventuali requisiti normativi specifici applicabili in funzione del settore di attività, della giurisdizione di appartenenza e dei servizi erogati.

5 IMPEGNO DELLA DIREZIONE

La sicurezza delle informazioni è una responsabilità gestionale e organizzativa e non esclusivamente tecnologica.
La Direzione del Gruppo Lutech riconosce la sicurezza come priorità strategica e si impegna a:

- garantire risorse adeguate alla protezione delle informazioni e degli asset informativi;
- definire ruoli, responsabilità e autorità in materia di sicurezza delle informazioni;
- promuovere una cultura aziendale orientata alla sicurezza, alla consapevolezza e alla responsabilizzazione del personale;
- assicurare un approccio sistematico alla gestione dei rischi per la sicurezza delle informazioni;
- perseguire il miglioramento continuo delle misure di sicurezza lungo l'intera catena del valore;
- assicurare la resilienza dei processi e dei servizi essenziali;
- considerare i rischi derivanti dalla catena di approvvigionamento e dalle terze parti;
- assicurare il rispetto delle disposizioni legislative, regolamentari, contrattuali e degli standard applicabili.

La Direzione promuove inoltre il monitoraggio dell'efficacia delle misure di sicurezza adottate e sostiene il continuo miglioramento del livello di protezione delle informazioni, in coerenza con l'evoluzione del contesto di rischio e degli obiettivi aziendali.

L'obiettivo del Gruppo Lutech è conseguire e mantenere un livello di sicurezza delle informazioni adeguato ai rischi, coerente con gli obiettivi aziendali e idoneo a supportare l'erogazione di servizi affidabili e resilienti.

l Gruppo assicura il rispetto delle disposizioni legislative, regolamentari e contrattuali applicabili, nonché degli standard adottati, promuovendo l'integrazione della sicurezza delle informazioni nei processi aziendali e nella gestione dei rapporti con clienti, fornitori e altre parti interessate.

6 ANALISI DEL CONTESTO E DELLE PARTI INTERESSATE

Il Gruppo Lutech analizza periodicamente il proprio contesto operativo, tecnologico e normativo, nonché delle aspettative delle parti interessate, tra cui clienti, fornitori, partner, autorità competenti, dipendenti e altre parti interessate rilevanti.

L'analisi del contesto consente di individuare i principali fattori di rischio e le opportunità di miglioramento, adottando misure di sicurezza proporzionate alla natura dei servizi erogati e con il livello di rischio accettabile.

Nell'analisi del contesto sono considerati anche i rischi fisici derivanti da eventi ambientali e climatici (es. fenomeni meteo estremi, interruzioni energetiche, ondate di calore, allagamenti), in quanto potenziali cause di indisponibilità di asset e servizi ICT e di interruzione dei processi di business.

7 PRINCIPI DI PROTEZIONE DELLE INFORMAZIONI

Il Gruppo Lutech assicura che le informazioni siano classificate in funzione del loro valore, della criticità e del livello di sensibilità, adottando adeguate misure di protezione per garantirne la riservatezza, l'integrità e la disponibilità.

Le informazioni e gli asset informativi sono gestiti durante l'intero ciclo di vita, dalla creazione o acquisizione fino alla dismissione, secondo criteri di classificazione, protezione, tracciabilità e conservazione, ove applicabile.

L'accesso alle informazioni ed ai sistemi informativi è consentito esclusivamente agli utenti autorizzati, secondo il principio del minimo privilegio e della segregazione delle funzioni.

Il Gruppo Lutech adotta misure tecniche e organizzative adeguate a prevenire accessi non autorizzati, divulgazioni indebite, alterazioni, perdite o distruzione delle informazioni, anche mediante l'impiego di tecniche di cifratura dei dati e delle comunicazioni, ove appropriato.

La sicurezza è considerata lungo l'intero ciclo di vita dei sistemi informativi, dalla progettazione o acquisizione fino alla manutenzione e alla dismissione, promuovendo l'adozione di requisiti di sicurezza fin dalle fasi iniziali e durante tutte le successive modifiche.

Le vulnerabilità di sicurezza degli asset e dei sistemi informativi sono identificate, valutate e trattate tempestivamente, in funzione del livello di rischio e dell'evoluzione delle minacce.

Il Gruppo Lutech assicura che le reti, le infrastrutture di comunicazione e i servizi di rete siano progettati, implementati, gestiti e monitorati secondo principi di sicurezza e resilienza, adottando misure tecniche e organizzative adeguate a prevenire accessi non autorizzati, intercettazioni, alterazioni, interruzioni dei servizi e altri eventi che possano comprometterne la sicurezza. Le reti e le comunicazioni sono monitorate al fine di rilevare tempestivamente anomalie, minacce e potenziali incidenti di sicurezza. Le modalità di progettazione, gestione, protezione e monitoraggio delle reti e delle comunicazioni sono disciplinate da procedure operative e standard tecnici adottati dal Gruppo, in funzione dei rischi e dei requisiti normativi applicabili.

Il Gruppo Lutech predispone e mantiene aggiornati piani di continuità operativa, di ripristino in caso di disastro e di gestione delle emergenze, al fine di assicurare la resilienza dei servizi e la continuità delle attività aziendali.

Gli eventi e gli incidenti di sicurezza, nonché le vulnerabilità identificate, sono tempestivamente segnalati, analizzati e gestiti secondo le disposizioni e le procedure adottate dal Gruppo.

8 GESTIONE DEL RISCHIO

La protezione delle informazioni si fonda su un approccio strutturato di gestione del rischio, finalizzato all'identificazione, all'analisi, alla valutazione e al trattamento dei rischi che possono compromettere la riservatezza, l'integrità e la disponibilità delle informazioni e degli asset informativi.

Le decisioni in materia di sicurezza delle informazioni tengono conto del contesto organizzativo, dell'evoluzione delle minacce, dell'impatto potenziale sui processi aziendali, sugli asset informativi e sui servizi erogati, adottando misure di sicurezza appropriate e proporzionate al livello di rischio.

La gestione del rischio considera anche i rischi derivanti dalla catena di approvvigionamento e dalle terze parti che, a qualsiasi titolo, trattano informazioni o accedono agli asset informativi del Gruppo Lutech.

9 SICUREZZA NEI SERVIZI CLOUD E PROTEZIONE DELLE INFORMAZIONI PERSONALI

Garantire il rispetto dei principi di legge sulla protezione dei dati e aumentare la fiducia dei clienti verso le tecnologie di cloud computing è un obiettivo strategico per il Gruppo Lutech. Il medesimo impegno riguarda specificatamente la protezione delle PII (Personally Identifiable information, ossia Dati Personali)

ovvero quello di fornire una modalità strutturata, basata sulla privacy by design, per far fronte alle principali questioni giuridiche, sia di natura legale che contrattuale, legate alla gestione dei dati personali in infrastrutture informatiche distribuite seguendo il modello del cloud pubblico. Il Gruppo Lutech integra tali principi nelle attività di progettazione, sviluppo, implementazione, monitoraggio e miglioramento dei servizi cloud, adottando controlli organizzativi e tecnici adeguati alla protezione delle informazioni personali.

10 OBIETTIVI E KPI

Il Gruppo Lutech definisce obiettivi in materia di sicurezza delle informazioni coerenti con la propria strategia aziendale e con il livello di rischio accettabile.

La Direzione identifica i seguenti obiettivi strategici a livello Gruppo:

- Proteggere le informazioni da accessi o divulgazioni (a seguito di azioni deliberate o per negligenza) non autorizzati;
- assicurare la classificazione delle informazioni in funzione del loro valore e del livello di sensibilità;
- garantire l'integrità delle informazioni, prevenendo modifiche non autorizzate;
- garantire la disponibilità delle informazioni e dei servizi a supporto dei processi aziendali;
- promuovere la formazione, la sensibilizzazione e la consapevolezza del personale in materia di sicurezza delle informazioni;
- gestire i rischi derivanti dalla catena di approvvigionamento, assicurando che fornitori e partner adottino misure di sicurezza adeguate ai servizi erogati;
- promuovere la tempestiva segnalazione, analisi e gestione degli eventi, degli incidenti di sicurezza e delle vulnerabilità.

Il raggiungimento degli obiettivi è monitorato mediante indicatori di prestazione (KPI) e ulteriori strumenti di monitoraggio definiti dal Gruppo e riesaminati periodicamente dalla Direzione.

11 SISTEMA DI GESTIONE E RESPONSABILITÀ

La sicurezza delle informazioni è supportata da un insieme coordinato di politiche, procedure, controlli tecnici e misure organizzative e processi di governance finalizzati a garantire un livello di protezione adeguato ai rischi e coerente con gli obiettivi del Gruppo.

Le Società del Gruppo sono tenute a conformare le loro attività in materia di sicurezza delle informazioni, alla normativa applicabile, al Sistema di Gestione per la Sicurezza delle Informazioni volontario ISO 27001 (o equivalente), a processi e procedure comuni al Gruppo Lutech.

Ruoli, responsabilità, autorità e livelli di accountability in materia di sicurezza delle informazioni sono formalmente definiti al fine di garantire efficaci processi decisionali, coordinamento, controllo e supervisione.

12 COMUNICAZIONE, FORMAZIONE E COINVOLGIMENTO

La Politica è comunicata a tutto il personale e agli altri soggetti che, a qualsiasi titolo, operano per conto delle Società del Gruppo o accedono alle informazioni e agli asset informativi

Il Gruppo Lutech promuove la formazione, la sensibilizzazione e la consapevolezza del proprio personale in materia di sicurezza delle informazioni, assicurando che i contenuti siano coerenti con i ruoli e le responsabilità assegnati.

Tutti i destinatari della presente Politica sono tenuti ad operare nel rispetto delle politiche, delle procedure e delle disposizioni di sicurezza del Gruppo, degli obblighi di riservatezza e delle responsabilità attribuite in funzione del ruolo ricoperto.

La consapevolezza, la responsabilizzazione e il coinvolgimento attivo di tutti i soggetti interessati costituiscono elemento essenziale per l'efficacia delle misure adottate.

13 CONFORMITÀ, MONITORAGGIO E MIGLIORAMENTO CONTINUO

Il Gruppo Lutech verifica periodicamente la conformità delle misure di sicurezza delle informazioni ai requisiti normativi, regolamentari, contrattuali e alle disposizioni interne applicabili.

A tal fine sono pianificate attività di monitoraggio, verifica ed audit della sicurezza delle informazioni, finalizzate a valutare l'efficacia delle misure adottate, individuare non conformità, aree di miglioramento e opportunità di rafforzamento del livello di sicurezza.

I risultati delle attività di verifica sono riportati alla Direzione affinché siano adottate le opportune decisioni e definite le azioni correttive e di miglioramento.

14 APPROVAZIONE, REVISIONE E VALIDITÀ

La Politica è soggetta a riesame periodico al fine di verificarne la continua adeguatezza rispetto all'evoluzione del contesto organizzativo, normativo, tecnologico e delle minacce alla sicurezza delle informazioni.

La Politica è inoltre aggiornata ogniqualvolta intervengano modifiche significative al contesto interno o esterno, ai requisiti applicabili, all'organizzazione o ai servizi del Gruppo Lutech che possano influire sulla sicurezza delle informazioni.

La Direzione promuove il periodico riesame dell'efficacia della presente Politica e ne assicura il mantenimento e il miglioramento continuo.

15 REQUISITI LOCALI

Le società del Gruppo Lutech sono tenute ad applicare la presente Politica nel rispetto delle leggi, dei regolamenti e delle disposizioni emanate dalle autorità competenti del Paese in cui operano.

Qualora la normativa locale preveda requisiti più restrittivi o ulteriori rispetto a quelli definiti nella presente Politica, tali requisiti prevalgono e devono essere recepiti attraverso procedure, standard o disposizioni locali.