POL-400

POLITICA DI SICUREZZA DELLE INFORMAZIONI

POLITICA

IDENTIFICAZIONE

Categoria:	SI - Sistema Sicurezza delle Informazioni		
Politica	POL-400 Politica di Sicurezza delle Informazioni		
Versione	07	**Del:**	27/03/2026

RESPONSABILITÀ

	Nome	**Funzione**
Elaborato da:	Flora Gallo	Compliance Officer
Verificato da:	Cristina Rossato	Chief Compliance Officer
Approvato da:	Giuseppe Di Franco	Chief Executive Officer

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.

INDICE

1 INTRODUZIONE

Il Patrimonio Informativo rappresenta la risorsa fondamentale per la gestione delle relazioni con i Clienti, per l'innovazione continua dell'offerta e per la qualità dei servizi erogati dal Gruppo Lutech. In quanto asset strategico, esso deve essere adeguatamente tutelato attraverso un costante bilanciamento tra il livello di rischio accettato e il grado di protezione richiesto, coniugando la tutela delle informazioni con l'efficienza, l'efficacia e la continuità dei processi di business.

In un contesto caratterizzato da crescente digitalizzazione, utilizzo esteso di sistemi informativi e coinvolgimento di un numero sempre maggiore di stakeholder, gli scenari di rischio evolvono rapidamente. La sicurezza delle informazioni assume pertanto un ruolo centrale nella protezione del valore aziendale e nella salvaguardia della reputazione del Gruppo Lutech.

2 SCOPO

La presente Politica definisce i principi e gli impegni adottati dal Gruppo Lutech per garantire la protezione delle informazioni 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 normative applicabili, degli obblighi contrattuali, delle richieste derivanti da audit di terze parti e da attività di due diligence, contribuendo alla continuità operativa e alla tutela degli interessi aziendali e dei clienti.

3 AMBITO DI APPLICAZIONE

La presente Politica si applica a tutte le Società del Gruppo Lutech, a tutto il personale, ai collaboratori, ai consulenti e ai fornitori coinvolti nelle attività aziendali, ai prodotti e servizi gestiti, e riguarda tutte le informazioni trattate dall'Organizzazione, indipendentemente dal formato o dal supporto utilizzato.

4 RIFERIMENTI NORMATIVI

- **ISO 27001:2022** - Information security, cybersecurity and privacy protection — Information security management systems — Requirements
- **ISO 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 27017:2015** - Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- **ISO 27018:2025** - Information security, cybersecurity and privacy protection — Guidelines for protection of personally identifiable information (PII) in public clouds acting as PII processors

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;
- definire ruoli e responsabilità chiare;
- promuovere una cultura aziendale orientata alla protezione delle informazioni;
- perseguire il miglioramento continuo delle misure di sicurezza lungo l'intera catena del valore.

L'obiettivo è conseguire e mantenere i più elevati livelli di qualità e sicurezza nei servizi erogati, assicurando che tali servizi non determinino un aumento dei rischi per i clienti.
L'Organizzazione assicura il pieno rispetto delle normative cogenti e volontarie (ove presenti), dei requisiti contrattuali applicabili ai servizi erogati e ai rapporti con clienti e fornitori, garantendo che le attività svolte non comportino un aumento dei rischi per le parti coinvolte.

6 ANALISI DEL CONTESTO E DELLE PARTI INTERESSATE

Il Gruppo Lutech tiene conto del proprio contesto operativo, tecnologico e normativo, nonché delle aspettative delle parti interessate, tra cui clienti, fornitori, partner, autorità e dipendenti.
L'analisi del contesto consente di individuare i principali fattori di rischio e di adottare misure di sicurezza proporzionate, coerenti con la 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

Le informazioni sono classificate in base al loro valore e livello di sensibilità e sono protette da accessi non autorizzati, anche mediante l'utilizzo di tecniche di cifratura dei dati e delle comunicazioni ove necessario.
Sono adottate misure tecniche e organizzative per prevenire divulgazioni indebite, alterazioni o perdite di dati e per garantire che le informazioni siano disponibili agli utenti autorizzati quando necessario.
Sono predisposti e mantenuti aggiornati piani di continuità operativa e di gestione delle emergenze. Tutti gli incidenti o potenziali vulnerabilità sono segnalati e analizzati secondo procedure definite.

8 GESTIONE DEL RISCHIO

La protezione delle informazioni si fonda su un approccio strutturato di identificazione, analisi e valutazione dei rischi. Le decisioni in materia di sicurezza tengono conto dell'impatto potenziale sugli asset informativi, delle aspettative delle parti interessate e della sostenibilità degli investimenti necessari alla mitigazione dei rischi.

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. Ciò riguarda espressamente le attività di progettazione, lo sviluppo, l'attuazione, il monitoraggio e la misurazione di politiche sulla privacy e controlli della privacy nei servizi di cloud computing.

10 OBIETTIVI E KPI

L'Organizzazione 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;
- Le informazioni siano opportunamente classificate;
- Le informazioni siano salvaguardate da modifiche non autorizzate, nel rispetto dell'integrità;
- Le informazioni siano sempre disponibili per gli usi consentiti;
- Il Personale riceva addestramento e aggiornamento sulla sicurezza delle informazioni;
- I Fornitori di tecnologie e di servizi correlati alla erogazione/gestione dei sistemi e dei servizi siano accuratamente selezionati e monitorati con i medesimi criteri e principi che LUTECH adotta per i propri processi interni;
- Tutte le violazioni della sicurezza delle informazioni e possibili punti deboli vengano riferiti a chi di dovere ed esaminati.

Assicura, inoltre, il monitoraggio di questi obiettivi attraverso la misurazione di Key Performance Indicator associati, come ad esempio la misurazione e il monitoraggio di:

- Personale formato su tematiche di sicurezza delle informazioni

- ❑ Audit a fornitori critici
- ❑ Incidenti di sicurezza delle Informazioni.

11 SISTEMA DI GESTIONE E RESPONSABILITÀ

La sicurezza delle informazioni è supportata da un insieme coordinato di politiche, procedure, controlli tecnici e misure organizzative.
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 e autorità sono formalmente definiti al fine di garantire coerenza, accountability e controllo lungo l'intera catena del valore.

12 COMUNICAZIONE, FORMAZIONE E COINVOLGIMENTO

La Politica è comunicata a tutto il personale e ai soggetti coinvolti nelle attività aziendali. Il personale deve ricevere formazione e aggiornamento periodico in materia di sicurezza delle informazioni.
La consapevolezza e il coinvolgimento attivo di tutti i soggetti interessati costituiscono elemento essenziale per l'efficacia delle misure adottate.

13 APPROVAZIONE, REVISIONE E VALIDITÀ

La presente Politica è soggetta a riesame periodico al fine di garantirne l'adeguatezza rispetto all'evoluzione del contesto organizzativo, normativo e tecnologico.
L'Organizzazione si impegna ad aggiornare la Politica ogni qualvolta intervengano cambiamenti significativi che possano influire sulla sicurezza delle informazioni.