LIKE DIGITAL SRL

P.IVA 02113250688

POLITICA INTEGRATA SECURITY

Politica per la Sicurezza delle Informazioni – ISO/IEC 27001:2022 § 5.2

Codice	LD-ISMS-POL-001 – All. B
Versione	1.0
Data emissione	10 Gennaio 2026
Emesso da	Alessandro De Florentiis
Norma	ISO/IEC 27001:2022

1. Scopo

La presente Politica Integrata per la Sicurezza delle Informazioni definisce l'orientamento strategico, gli obiettivi e i principi guida che Like Digital SRL adotta per proteggere le informazioni proprie e dei propri clienti.

Il documento è emesso dalla Direzione ai sensi del punto 5.2 della norma ISO/IEC 27001:2022 e costituisce il riferimento di primo livello per l'intero Sistema di Gestione della Sicurezza delle Informazioni (SGSI).

2. Campo di applicazione

La presente politica si applica a:

- Tutte le risorse umane di Like Digital SRL: dipendenti, collaboratori, consulenti, tirocinanti;
- Tutti i sistemi informativi, le infrastrutture tecnologiche e i dati trattati nell'ambito delle attività aziendali;
- I processi di sviluppo software, assistenza clienti, gestione commerciale, approvvigionamento e gestione risorse;
- I fornitori e i partner che accedono, trattano o gestiscono informazioni per conto di Like Digital SRL.

3. Contesto organizzativo

Like Digital SRL è un'azienda operante nel settore dello Sviluppo Software e dei Servizi IT, con sede in Italia. Le informazioni trattate includono dati tecnici, dati di progetto, dati personali dei clienti (soggetti alle disposizioni del GDPR – Reg. UE 679/2016), codice sorgente proprietario e documentazione contrattuale.

In tale contesto, la sicurezza delle informazioni rappresenta un fattore abilitante per la fiducia dei clienti, la continuità operativa e il rispetto degli obblighi normativi.

4. Dichiarazione della Direzione

La Direzione di Like Digital SRL dichiara il proprio impegno a:

01	Garantire la riservatezza, l'integrità e la disponibilità delle informazioni aziendali e dei clienti.
02	Stabilire, attuare, mantenere e migliorare continuamente il SGSI in conformità alla norma ISO/IEC 27001:2022.
03	Definire e perseguire obiettivi misurabili per la sicurezza delle informazioni, riesaminati almeno annualmente.
04	Assicurare le risorse (umane, tecnologiche, economiche) necessarie al corretto funzionamento del SGSI.
05	Sensibilizzare e formare tutto il personale sui temi della sicurezza delle informazioni.
06	Rispettare tutti i requisiti legali, normativi e contrattuali applicabili, incluso il GDPR.
07	Gestire i rischi per la sicurezza delle informazioni in modo sistematico e documentato.
08	Garantire la continuità operativa e la capacità di risposta agli incidenti di sicurezza.
09	Promuovere una cultura della sicurezza a tutti i livelli dell'organizzazione.
10	Valutare e gestire i rischi connessi ai fornitori e alla catena di approvvigionamento IT.

5. Principi fondamentali della sicurezza

5.1 Triade CIA

Il SGSI di Like Digital SRL è fondato sui tre pilastri fondamentali della sicurezza delle informazioni:

RISERVATEZZA
Le informazioni sono accessibili solo a soggetti autorizzati. Gli accessi sono regolati da profili e privilegi minimi necessari (least privilege).

INTEGRITÀ
Le informazioni sono accurate, complete e protette da modifiche non autorizzate. L'integrità è garantita da controlli tecnici e procedurali.

DISPONIBILITÀ
Le informazioni e i sistemi sono accessibili ai soggetti autorizzati quando necessario, garantendo la continuità del servizio.

5.2 Principi operativi

- Need-to-know e least privilege: ogni utente accede solo alle informazioni strettamente necessarie al proprio ruolo;
- Separazione dei compiti (Segregation of Duties): le attività critiche sono suddivise tra soggetti distinti;
- Defense in depth: misure di sicurezza stratificate (fisiche, logiche, procedurali) per ridurre la superficie d'attacco;
- Security by design: la sicurezza è integrata nei processi di sviluppo software fin dalla fase di progettazione;
- Zero Trust: nessun accesso è considerato implicitamente sicuro, indipendentemente dalla rete di provenienza;
- Gestione proattiva dei rischi: identificazione, valutazione e trattamento sistematici dei rischi per la sicurezza.

6. Obiettivi della sicurezza delle informazioni

Gli obiettivi specifici sono definiti nel documento 'Pianificazione Obiettivi' e riesaminati in occasione del Riesame della Direzione. A titolo esemplificativo e non esaustivo:

Obiettivo	Indicatore (KPI)	Target

Ridurre gli incidenti di sicurezza	*N. incidenti segnalati/anno*	**< 5**
Garantire la formazione del personale	*% dipendenti formati*	**100%**
Completare gli audit interni pianificati	*Audit completati / pianificati*	**100%**
Gestione vulnerabilità critica	*Tempo medio di patching (giorni)*	**< 30 gg**
Continuità operativa	*RTO / RPO sistemi critici*	**< 4h / < 24h**

7. Ruoli e responsabilità

Ruolo	Responsabilità principali
Direzione / RDD (Alessandro De Florentiis)	Approvazione della politica e del SGSI, definizione obiettivi, allocazione risorse, riesame direzionale.
RGQS (Manuela De Florentiis)	Coordinamento del SGSI, supervisione audit, monitoraggio KPI, gestione non conformità.
Responsabili di processo	Attuazione dei controlli nell'area di competenza, segnalazione di incidenti e non conformità.
Tutto il personale	Rispetto delle politiche e procedure di sicurezza, partecipazione alla formazione, segnalazione di eventi sospetti.
Fornitori / Partner	Rispetto delle clausole contrattuali di sicurezza e delle procedure applicabili.

8. Gestione dei rischi

Like Digital SRL adotta un processo strutturato di gestione del rischio per la sicurezza delle informazioni, basato sulla norma ISO/IEC 27005 e documentato nel documento PS.04 – Piano Analisi e Trattamento Rischio. Il processo prevede:

- Identificazione degli asset informativi e delle minacce potenziali;
- Valutazione della probabilità e dell'impatto di ciascun rischio;
- Definizione delle opzioni di trattamento: riduzione, accettazione, trasferimento, eliminazione;
- Implementazione dei controlli selezionati dall'Annex A della norma;
- Monitoraggio periodico e riesame dell'efficacia dei trattamenti adottati.

9. Conformità normativa

Like Digital SRL si impegna a rispettare tutti i requisiti normativi, regolamentari e contrattuali applicabili. I principali riferimenti normativi includono:

- ISO/IEC 27001:2022 – Norma di certificazione del SGSI;
- ISO/IEC 27002:2022 – Linee guida per i controlli di sicurezza;
- Regolamento UE 679/2016 (GDPR) – Protezione dei dati personali;
- D.Lgs. 196/2003 e s.m.i. – Codice Privacy italiano;
- Direttiva NIS2 (UE 2022/2555) – Sicurezza delle reti e dei sistemi informativi;
- Standard PCI-DSS (ove applicabile) – Sicurezza dei dati di pagamento.

10. Comunicazione e divulgazione

La presente politica è:

- Pubblicata e accessibile a tutto il personale tramite il sistema di gestione documentale aziendale;
- Illustrata ai nuovi assunti nell'ambito dell'onboarding;
- Condivisa con i fornitori e i partner rilevanti tramite contratto o apposita comunicazione;
- Disponibile alle parti interessate esterne su richiesta, nella versione approvata per la divulgazione.

11. Riesame e aggiornamento

La presente politica è riesaminata almeno annualmente, in occasione del Riesame della Direzione, o a seguito di:

- Significative modifiche al contesto organizzativo, tecnologico o normativo;
- Incidenti di sicurezza di rilievo;
- Esito di audit interni o esterni;
- Cambiamenti nel panorama delle minacce informatiche.

La revisione è documentata nel Verbale di Riesame della Direzione (RDD).

12. Approvazione

Ruolo	Nome	Firma e Data
Rappresentante della Direzione (RDD)	Alessandro De Florentiis	
Responsabile RGQS	Manuela De Florentiis