# Politica di sicurezza delle informazioni

**Organizzazione:** SparkFabrik S.r.l.
**Revisione:** 1.0
**Data emissione:** 22 ottobre 2025

## Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali.

## Campo di Applicazione

La presente "POL Politica di sicurezza delle informazioni" definisce gli obiettivi strategici, i principi fondamentali e l'impegno della Direzione di SparkFabrik per la protezione degli asset informativi. Questo documento costituisce il quadro di riferimento per il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), in conformità con gli standard internazionali ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018. La politica si applica a tutto il personale, ai collaboratori, ai processi e alle tecnologie che rientrano nel campo di applicazione del SGSI, con l'obiettivo di garantire la riservatezza, l'integrità e la disponibilità delle informazioni proprie e di quelle affidate dai clienti.

## Riferimenti Normativi

- **ISO/IEC 27001:2022**: Sistemi di gestione per la sicurezza delle informazioni — Requisiti.
- **ISO/IEC 27017:2015**: Codice di buone pratiche per i controlli di sicurezza delle informazioni per i servizi cloud.
- **ISO/IEC 27018:2019**: Codice di buone pratiche per la protezione delle informazioni personali (PII) nei cloud pubblici che agiscono come responsabili del trattamento di PII.
- **Regolamento (UE) 2016/679 (GDPR)**: Regolamento generale sulla protezione dei dati.

## Termini e Definizioni

- **Disponibilità**: La proprietà di essere accessibile e utilizzabile su richiesta da un'entità autorizzata.
- **Integrità**: La proprietà di accuratezza e completezza.
- **Informazioni Personali Identificabili (PII)**: Qualsiasi informazione che possa essere utilizzata, da sola o in combinazione con altre informazioni, per identificare un individuo.
- **Riservatezza**: La proprietà che l'informazione non sia resa disponibile o divulgata a persone, entità o processi non autorizzati.
- **Sistema di Gestione della Sicurezza delle Informazioni (SGSI)**: Parte del sistema di gestione complessivo, basato su un approccio al rischio aziendale, per stabilire, implementare, rendere operativo, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.

## Ruoli e Responsabilità

- **Top Management**: Definisce gli indirizzi strategici per la sicurezza delle informazioni, approva la relativa politica, assicura la disponibilità delle risorse necessarie e promuove una cultura della sicurezza a tutti i livelli aziendali.
- **CEO**: Guida l'impegno del Top Management verso la sicurezza delle informazioni e ha la responsabilità ultima della strategia complessiva e della governance aziendale, inclusa la definizione della politica di sicurezza.
- **RSGSI (Responsabile del Sistema di Gestione della Sicurezza delle Informazioni)**: Assicura l'implementazione, il mantenimento e il miglioramento continuo del SGSI. Coordina le attività di conformità, supervisiona la gestione dei rischi e degli incidenti e riferisce al Top Management sulle prestazioni del sistema.

## Obiettivi di sicurezza delle informazioni

Il Top Management di SparkFabrik si impegna a perseguire i seguenti obiettivi strategici per la sicurezza delle informazioni, assicurando che il Sistema di Gestione della Sicurezza delle Informazioni (SGSI) sia allineato con il contesto e gli indirizzi strategici dell'azienda:

- **Protezione degli Asset Informativi**: Garantire la riservatezza, l'integrità e la disponibilità di tutte le informazioni e degli asset informativi di proprietà di SparkFabrik e dei suoi clienti. La protezione è attuata in base alla classificazione e alla criticità degli asset, come definito nella "POL Politica di classificazione ed etichettatura delle informazioni".
- **Gestione dei Rischi**: Adottare un approccio sistematico e continuo basato sul rischio per identificare, valutare, trattare e monitorare le minacce alla sicurezza delle informazioni. Le misure di controllo devono essere adeguate e proporzionate ai rischi identificati, secondo le modalità descritte nella "PRO Procedura di gestione dei rischi".
- **Conformità Normativa e Contrattuale**: Assicurare la piena conformità con tutti i requisiti legali, normativi, statutari e contrattuali applicabili alle attività di SparkFabrik. Un'attenzione

particolare è rivolta alla protezione dei dati personali (PII) in accordo con la legislazione vigente, i cui principi sono stabiliti nella "POL Politica di protezione delle PII".
- **Sicurezza nel Cloud Computing**: Gestire in modo sicuro i servizi cloud, sia in qualità di fornitore per i propri clienti sia come fruitore di servizi di terze parti. Questo obiettivo si realizza applicando un modello di responsabilità condivisa e implementando i controlli specifici dettagliati nella "POL Politica di sicurezza del cloud".
- **Miglioramento Continuo**: Promuovere il miglioramento continuo del SGSI attraverso attività di monitoraggio, audit periodici e riesami da parte della Direzione. Il RSGSI ha la responsabilità di riferire al Top Management sulle prestazioni del sistema, come formalizzato nella "PRO Gestione riesame della direzione", per garantirne la costante adeguatezza ed efficacia.

## Principi fondamentali di sicurezza delle informazioni

Per raggiungere gli obiettivi prefissati, SparkFabrik adotta i seguenti principi fondamentali che guidano le decisioni e le azioni in materia di sicurezza delle informazioni:

- **Leadership e Impegno della Direzione**: Il Top Management, con la guida del CEO, deve dimostrare un impegno attivo e visibile verso la sicurezza delle informazioni. Tale impegno si manifesta attraverso l'approvazione della presente politica, l'allocazione delle risorse necessarie e la promozione di una cultura della sicurezza a tutti i livelli aziendali.
- **Responsabilità Condivisa e Consapevolezza**: La sicurezza delle informazioni è una responsabilità di tutto il personale. Ogni dipendente e collaboratore è tenuto a comprendere e rispettare le politiche e le procedure del SGSI. L'adesione ai principi di sicurezza è un dovere professionale, come richiamato anche nel "Codice di condotta".
- **Definizione di Ruoli e Responsabilità**: Le responsabilità relative alla sicurezza delle informazioni sono formalmente definite, assegnate e comunicate a tutti i livelli dell'organizzazione. Il RSGSI assicura che tali responsabilità siano chiaramente integrate nei ruoli aziendali, in coerenza con quanto stabilito nella "POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni".
- **Uso Accettabile delle Risorse Aziendali**: Tutto il personale deve utilizzare le informazioni e gli asset associati, inclusi sistemi, reti e dispositivi, in modo responsabile, etico e conforme alle regole definite nella "POL Politica di sicurezza operativa".
- **Sicurezza negli Ambienti Cloud**:
    - In qualità di fornitore di servizi cloud, SparkFabrik deve implementare e mantenere controlli robusti per garantire l'isolamento degli ambienti dei clienti (multi-tenancy), la sicurezza degli accessi ai loro dati da parte del personale autorizzato e la gestione sicura del ciclo di vita degli account.
    - In qualità di cliente di servizi cloud, SparkFabrik deve valutare e gestire i rischi associati ai fornitori terzi, con particolare attenzione alla localizzazione geografica dei dati e alla chiara definizione delle responsabilità contrattuali.

    - Le direttive operative per entrambi gli scenari sono dettagliate nella "POL Politica di sicurezza del cloud".
- **Protezione dei Dati Personali (PII)**: SparkFabrik si impegna a proteggere i dati personali trattati per conto dei clienti, agendo in qualità di Responsabile del Trattamento, e i propri dati aziendali, in piena conformità con la legislazione vigente. Le responsabilità per la protezione delle PII sono chiaramente definite negli accordi contrattuali con i clienti, come specificato nella "POL Politica di protezione delle PII".
- **Sicurezza dell'Ambiente di Lavoro Fisico e Remoto**:
    - Tutto il personale deve adottare le pratiche di "scrivania pulita e schermo pulito", proteggendo i documenti cartacei e i supporti di memorizzazione rimovibili e assicurando il blocco delle sessioni di lavoro quando la postazione è incustodita.
    - Gli asset aziendali utilizzati al di fuori delle sedi (telelavoro) devono essere protetti da furto, perdita o accessi non autorizzati. È fatto divieto di svolgere attività lavorative in luoghi pubblici o non sicuri che possano compromettere la riservatezza delle informazioni.
- **Segnalazione degli Eventi di Sicurezza**: Tutto il personale ha l'obbligo di segnalare tempestivamente qualsiasi evento, incidente o vulnerabilità di sicurezza, sia sospetto che confermato, attraverso i canali appropriati e seguendo la "PRO Procedura di gestione degli incidenti di sicurezza delle informazioni".
- **Governo e Revisione delle Politiche**: La presente politica e i documenti ad essa collegati sono soggetti a revisione periodica, e comunque ogni qualvolta si verifichino cambiamenti significativi. Il RSGSI coordina il processo di revisione, mentre il Top Management approva formalmente ogni aggiornamento per garantirne la continua idoneità, adeguatezza ed efficacia.

## Archiviazione e Aggiornamenti

Questo documento è gestito all'interno del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) ed è archiviato in formato controllato. Viene sottoposto a revisione con cadenza almeno annuale, o a seguito di cambiamenti organizzativi, tecnologici o normativi rilevanti, per assicurarne la costante adeguatezza. Ogni aggiornamento è formalmente approvato dal Top Management.

## Documenti di Riferimento

- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di gestione dei rischi
- POL Politica di protezione delle PII
- POL Politica di sicurezza del cloud
- PRO Gestione riesame della direzione
- Codice di condotta
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni

- POL Politica di sicurezza operativa
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni