POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	16/03/2026	Alessandro De Faveri	Alessandro De Faveri

Indice

Scopo

NODOPIANO DI ALESSANDRO DE FAVERI & C. S.a.s. adotta la presente politica quale espressione dell'impegno del Top Management a governare il Sistema di Gestione della Sicurezza delle Informazioni in modo coerente con la propria missione — unire tecnologia e creatività per connettere le imprese ai propri clienti — e con gli indirizzi strategici dello studio digitale.

Il documento traduce la visione dell'organizzazione in principi, impegni e obiettivi che orientano tutte le attività di protezione degli asset informativi, assicurando che la sicurezza delle informazioni sia parte integrante della cultura aziendale, dei processi operativi e delle relazioni con clienti B2B, enti pubblici, consorzi e partner. Attraverso questa politica, l'organizzazione intende garantire che il sistema di gestione resti appropriato al proprio contesto, al modello di business e all'evoluzione del panorama delle minacce, sostenendo al contempo la creazione di valore e la fiducia delle parti interessate.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi gestiti presso la sede operativa di Via Cal de Formiga, 12/D – 32035 Santa Giustina (BL), nonché in qualsiasi contesto di lavoro remoto o in trasferta. Coinvolge l'intero personale dell'organizzazione, i collaboratori esterni, i consulenti e le terze parti che accedono alle informazioni o ai sistemi aziendali. Rientrano nel perimetro i servizi di sviluppo web e software, web hosting, brand strategy, social media e advertising erogati a clienti B2B e istituzionali. Sono esclusi dal presente documento i requisiti operativi di dettaglio, disciplinati dalle politiche e procedure specifiche del Sistema di Gestione.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- GDPR

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Sistema di gestione della sicurezza delle informazioni (SGSI)** : insieme di politiche, procedure, processi e risorse utilizzati per dirigere e controllare le attività di sicurezza delle informazioni dell'organizzazione.
- **Riservatezza** : proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di accuratezza e completezza delle informazioni.

- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso come combinazione della probabilità di un evento e delle sue conseguenze.
- **Asset** : qualsiasi elemento che abbia valore per l'organizzazione, inclusi informazioni, software, hardware, servizi e risorse umane.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata da, o percepire di essere influenzata da una decisione o attività.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni del sistema di gestione.

Ruoli e responsabilità

- **Datore di Lavoro** : approva la presente politica, assicura la disponibilità delle risorse necessarie al SGSI e promuove il miglioramento continuo della sicurezza delle informazioni.
- **RSG (Responsabile del Sistema di Gestione)** : coordina l'attuazione, il mantenimento e il miglioramento continuo del SGSI, pianifica gli audit interni e prepara i report per il riesame della direzione.
- **Responsabile Sviluppo Software / Technical Lead / Responsabile IT** : gestisce i controlli tecnici di sicurezza sull'infrastruttura IT, sui servizi di hosting e sugli ambienti di sviluppo.
- **Responsabile Privacy** : garantisce la conformità dei trattamenti di dati personali alla normativa vigente e gestisce le violazioni dei dati.
- **Tutto il personale e le terze parti autorizzate** : aderisce alle politiche e procedure del SGSI, segnala tempestivamente gli eventi di sicurezza e custodisce con diligenza gli asset assegnati.

Impegno e obiettivi del sistema di gestione

Impegno del Top Management

L'organizzazione riconosce nella sicurezza delle informazioni un fattore abilitante per la qualità dei servizi digitali e per la fiducia che clienti, enti pubblici e partner ripongono nello studio. Il **Datore di Lavoro** , in qualità di vertice decisionale, si impegna a:

- assicurare che la presente politica e gli obiettivi di sicurezza restino appropriati al contesto di NODOPIANO, al suo modello di business e all'evoluzione del panorama delle minacce;
- garantire l'integrazione dei requisiti di sicurezza delle informazioni nei processi operativi dello studio — dallo sviluppo software al web hosting, dalla comunicazione digitale alla gestione dei dati dei clienti;

- mettere a disposizione le risorse umane, tecnologiche e finanziarie necessarie a sostenere il SGSI;
- promuovere una cultura in cui ogni collaboratore contribuisca attivamente alla protezione degli asset informativi.

Principi fondamentali

La politica si fonda su principi che permeano l'intera organizzazione e guidano ogni decisione in materia di sicurezza:

- **Approccio basato sul rischio** — l'organizzazione valuta sistematicamente la probabilità e l'impatto degli eventi avversi, applicando controlli proporzionati al livello di rischio accettabile.
- **Responsabilità condivisa** — ogni dipendente, collaboratore esterno e terza parte è responsabile dell'uso corretto delle risorse assegnate e del rispetto delle regole di sicurezza.
- **Classificazione e trattamento delle informazioni** — le informazioni sono classificate in base alla loro sensibilità e valore; a ciascun livello corrispondono requisiti di protezione specifici per il trattamento, la trasmissione e la conservazione.
- **Uso accettabile delle risorse** — regole chiare disciplinano l'accesso, l'utilizzo e la restituzione degli asset aziendali, con assegnazione formale e tracciabilità.
- **Segnalazione degli eventi di sicurezza** — canali efficaci garantiscono la tempestiva comunicazione di qualsiasi evento o sospetta violazione di sicurezza.
- **Protezione dell'ambiente di lavoro** — misure quali la politica di schermo e scrivania puliti e il blocco automatico dei dispositivi prevengono l'accesso non autorizzato alle informazioni.
- **Miglioramento continuo** — l'organizzazione riesamina e perfeziona con regolarità i controlli di sicurezza, i risultati degli audit interni e le lezioni apprese, così da accrescere nel tempo l'efficacia del SGSI e la propria capacità di risposta alle minacce emergenti.

Obiettivi di sicurezza delle informazioni

L'organizzazione persegue i seguenti obiettivi strategici, misurati e riesaminati in sede di riesame della direzione:

- garantire la **riservatezza** del codice sorgente, dei dati dei clienti e delle informazioni strategiche, limitando l'accesso sulla base del principio di necessità;
- preservare l' **integrità** delle informazioni nelle attività di sviluppo software, hosting e comunicazione digitale;
- assicurare la **disponibilità** dei sistemi e dei servizi IT in linea con le esigenze operative e gli impegni contrattuali verso i clienti B2B e istituzionali;
- ridurre l'esposizione al rischio di sicurezza attraverso la valutazione periodica delle minacce e l'adozione di misure di trattamento proporzionate;

- promuovere la consapevolezza del personale affinché ogni membro dell'organizzazione contribuisca attivamente alla protezione degli asset;
- assicurare la conformità ai requisiti normativi e contrattuali applicabili, incluse le disposizioni in materia di protezione dei dati personali.

Impegno alla conformità e al miglioramento

L'organizzazione si impegna a soddisfare tutti i requisiti applicabili relativi alla sicurezza delle informazioni — siano essi di natura legale, regolamentare, contrattuale o derivanti dalle aspettative delle parti interessate — e a perseguire il miglioramento continuo del SGSI. Tale impegno si traduce nell'adozione di un ciclo strutturato di pianificazione, attuazione, verifica e riesame che consente di adattare progressivamente il sistema di gestione alle nuove condizioni operative e all'evoluzione del contesto.

Comunicazione della politica

La presente politica è resa disponibile come informazione documentata del SGSI. Viene comunicata a tutto il personale interno e, ove opportuno, alle parti interessate esterne attraverso i canali stabiliti nella *PRO Procedura gestione comunicazione* . La classificazione del documento è "public", al fine di favorirne la massima accessibilità e trasparenza.

Archiviazione e aggiornamento

La presente politica è archiviata e gestita in conformità alla *PRO Procedura di gestione delle informazioni documentate* . Il **RSG (Responsabile del Sistema di Gestione)** ne cura la revisione con cadenza annuale oppure a seguito di cambiamenti significativi nel contesto organizzativo, tecnologico o nel panorama delle minacce. Ogni revisione è sottoposta all'approvazione del **Datore di Lavoro** prima della pubblicazione e della comunicazione al personale e alle parti interessate.

Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura gestione comunicazione
- PRO Processi direzionali
- PRO Gestione riesame della direzione