POL Politica di sicurezza delle informazioni

Storia della versione

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

Indice

Scopo

La presente politica formalizza l'impegno del **Datore di Lavoro** , nella sua funzione di vertice organizzativo, verso la protezione sistematica degli asset informativi di NODOPIANO DI ALESSANDRO DE FAVERI & C. S.a.s. Il documento costituisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), con l'obiettivo di salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito dei servizi di sviluppo software, web hosting, comunicazione digitale e consulenza IT offerti dall'organizzazione.

Attraverso questa politica, l'organizzazione intende assicurare che la sicurezza delle informazioni sia integrata nei processi aziendali e nelle decisioni strategiche, sostenendo la fiducia dei clienti B2B e istituzionali e tutelando il patrimonio informativo quale risorsa critica per la continuità del business.

Campo di applicazione

La 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. Sono esclusi dal perimetro del presente documento i requisiti operativi di dettaglio, disciplinati dalle politiche e procedure specifiche richiamate nella sezione Documenti di riferimento.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Regolamento (UE) 2016/679

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.
- **Evento di sicurezza delle informazioni** : occorrenza identificata in un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza o un malfunzionamento dei controlli.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni che, con significativa probabilità, compromettono le operazioni aziendali e minacciano la sicurezza delle informazioni.

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 e conduce 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.

Obiettivi di sicurezza delle informazioni

L'organizzazione persegue obiettivi di sicurezza coerenti con la propria missione di studio digitale e web agency, orientati alla tutela del patrimonio informativo e alla soddisfazione dei requisiti dei clienti e delle parti interessate. In particolare, NODOPIANO si impegna a:

- garantire la riservatezza del codice sorgente, dei dati dei clienti e delle informazioni strategiche, limitando l'accesso al personale autorizzato sulla base del principio di necessità operativa;
- preservare l'integrità delle informazioni trattate nei progetti di sviluppo software, nei servizi di hosting e nelle attività di comunicazione digitale, prevenendo alterazioni non

autorizzate;

- 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 ai rischi di sicurezza attraverso la valutazione periodica delle minacce e l'attuazione di misure di trattamento proporzionate al livello di rischio individuato;
- promuovere la consapevolezza del personale in materia di sicurezza delle informazioni, affinché ciascun membro dell'organizzazione contribuisca attivamente alla protezione degli asset;
- assicurare la conformità ai requisiti normativi e contrattuali applicabili, inclusi quelli derivanti dalla protezione dei dati personali.

Principi fondamentali di sicurezza delle informazioni

L'organizzazione fonda il proprio Sistema di Gestione della Sicurezza delle Informazioni su un insieme di principi che orientano ogni decisione, controllo e comportamento in materia di protezione degli asset informativi.

Approccio basato sul rischio. NODOPIANO adotta una gestione sistematica dei rischi per la sicurezza delle informazioni, valutando la probabilità e l'impatto degli eventi avversi e determinando le misure di trattamento in proporzione al livello di rischio individuato. Tale approccio consente di allocare le risorse là dove il beneficio in termini di protezione risulta più significativo e di adattare i controlli all'evoluzione del contesto tecnologico e delle minacce.

Responsabilità condivisa. La protezione delle informazioni non è circoscritta a una singola funzione: ogni membro del personale, ogni collaboratore esterno e ogni terza parte che accede ai sistemi aziendali è responsabile dell'uso corretto delle risorse assegnate e del rispetto delle regole stabilite dal SGSI. L'organizzazione promuove una cultura in cui la sicurezza è integrata nelle attività quotidiane di ciascuno.

Classificazione e trattamento delle informazioni. Le informazioni sono classificate in funzione della loro sensibilità e del valore che rivestono per l'organizzazione, e a ciascun livello di classificazione corrispondono requisiti specifici di protezione durante il trattamento, la trasmissione e la conservazione. Questo principio garantisce che i controlli siano proporzionati alla criticità dell'informazione.

Uso accettabile delle risorse. L'organizzazione definisce regole chiare sull'uso delle informazioni e degli asset associati, affinché il personale comprenda le proprie prerogative e i propri limiti nell'accesso, nell'utilizzo e nella restituzione delle risorse aziendali. L'assegnazione formale dei beni e la documentazione degli utenti autorizzati assicurano trasparenza e tracciabilità.

Segnalazione degli eventi di sicurezza. L'organizzazione predispone canali efficaci affinché il personale possa comunicare senza ritardo qualsiasi evento o sospetto di violazione della sicurezza delle informazioni. Una segnalazione tempestiva è condizione indispensabile per contenere gli impatti e avviare le attività di risposta e di analisi.

Protezione dell'ambiente di lavoro. L'organizzazione adotta misure per tutelare la riservatezza delle informazioni anche nello spazio fisico, attraverso regole di scrivania e schermo liberi da informazioni sensibili e il blocco automatico dei dispositivi durante i periodi di inattività, al fine di prevenire accessi non autorizzati e visualizzazioni indebite.

Miglioramento continuo. L'organizzazione si impegna a riesaminare e perfezionare con regolarità i controlli di sicurezza, i risultati delle verifiche interne e le lezioni apprese dagli eventi, così da accrescere nel tempo l'efficacia del SGSI e la propria capacità di risposta alle minacce emergenti.

Protezione degli asset fuori sede

L'organizzazione riconosce che una parte significativa delle attività lavorative si svolge al di fuori della sede di Santa Giustina, in modalità di lavoro remoto o durante trasferte presso i clienti. In tali contesti, i dispositivi e le informazioni aziendali restano soggetti ai medesimi requisiti di protezione vigenti in sede, e l'organizzazione si impegna a garantirne la sicurezza attraverso i seguenti principi.

Custodia e sorveglianza. I dispositivi aziendali — notebook, smartphone, tablet e supporti di memorizzazione — non sono mai lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di strutture ricettive o spazi di coworking. Il personale assegnatario li custodisce sotto il proprio diretto controllo oppure li ripone in luogo chiuso a chiave. La postazione di lavoro remoto è configurata in modo da impedire a persone non autorizzate, inclusi familiari o coinquilini, di visualizzare lo schermo o accedere ai dispositivi.

Connettività sicura. Il collegamento ai sistemi aziendali da postazioni esterne avviene esclusivamente tramite reti cifrate con standard almeno WPA2; l'uso di reti Wi-Fi aperte o non protette è vietato per qualsiasi trattamento di informazioni aziendali. Per l'accesso alle risorse interne è richiesto l'utilizzo della VPN aziendale, e le credenziali predefinite del router domestico devono essere sostituite prima dell'uso.

Segnalazione di smarrimento, furto o danneggiamento. Il personale notifica immediatamente al **Responsabile Sviluppo Software / Technical Lead / Responsabile IT** qualsiasi smarrimento, furto o danneggiamento di un asset aziendale fuori sede. In caso di furto, l'assegnatario presenta denuncia alle autorità competenti e informa contestualmente l'organizzazione affinché siano attivate le procedure di blocco remoto, revoca degli accessi e sostituzione delle credenziali. L'evento è registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni* .

Restituzione degli asset. Al termine del rapporto di lavoro, del progetto o dell'incarico, l'assegnatario restituisce integralmente i beni ricevuti. L'assegnazione e la riconsegna sono formalizzate attraverso il *MOD Modulo di assegnazione dei beni* , che documenta le condizioni d'uso e gli obblighi di custodia.

Comunicazioni riservate. Le comunicazioni che coinvolgono informazioni riservate o limitate sono effettuate esclusivamente attraverso i canali approvati dall'organizzazione; l'uso di applicazioni di messaggistica personali o di account e-mail non aziendali per la trasmissione di dati sensibili non è consentito.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGSI, archiviato e gestito secondo le modalità definite nella *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 operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di gestione dei rischi
- MOD Registro degli incidenti di sicurezza delle informazioni
- MOD Modulo di assegnazione dei beni