POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	07/05/2026	Miriam Magni	Domenico Pontieri

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Obiettivi di sicurezza delle informazioni
- Principi fondamentali di sicurezza delle informazioni
- Protezione degli asset fuori sede
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

La presente politica formalizza l'impegno del Top Management di Dr.Feel Srl verso la protezione del patrimonio informativo aziendale e rappresenta il documento quadro del Sistema di Gestione della Sicurezza delle Informazioni (SGSI), componente del Sistema di Gestione Integrato (SGI) adottato dall'organizzazione. Attraverso questa politica, Dr.Feel Srl dichiara la propria volontà di istituire, attuare, mantenere e migliorare continuamente un insieme coerente di politiche, processi e controlli finalizzati a salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni.

In qualità di struttura sanitaria autorizzata e fornitore di soluzioni di sanità digitale e telemedicina, l'organizzazione riconosce che la fiducia di pazienti, clienti corporate e parti interessate dipende dalla capacità di proteggere i dati sanitari, personali e aziendali trattati attraverso la piattaforma Dr.Feel e il poliambulatorio di Milano. La presente politica stabilisce pertanto il quadro di riferimento entro cui si inseriscono tutte le politiche tematiche, le procedure operative e i controlli di sicurezza delle informazioni, in coerenza con gli obiettivi strategici aziendali e con il contesto normativo applicabile. Il Top Management si impegna affinché questa politica sia comunicata a tutto il personale interessato e alle parti interessate rilevanti, resa accessibile e riesaminata a intervalli pianificati per garantirne la continua adeguatezza.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici di Dr.Feel Srl, inclusa la sede operativa di Via Colonnetta 5, 20122 Milano (MI), nonché gli ambienti di lavoro da remoto utilizzati dal personale. Coinvolge tutti i dipendenti, i collaboratori, i consulenti e le terze parti che accedono alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro adottata.

Riferimenti normativi

- ISO/IEC 27001:2022
- ISO/IEC 27002:2022
- Reg. (UE) 2016/679
- D.Lgs. 196/2003

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **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.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa allo stato di un sistema, servizio o rete che indica una possibile violazione della politica di sicurezza delle informazioni, un fallimento dei controlli o una situazione precedentemente sconosciuta potenzialmente rilevante per la sicurezza.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.
- **Asset** : qualsiasi elemento che abbia valore per l'organizzazione.
- **Controllo** : misura che modifica il rischio.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata da o percepirsi influenzata da una decisione o attività.

Ruoli e responsabilità

- **Direzione** : approva la presente politica e garantisce la disponibilità delle risorse necessarie alla sicurezza delle informazioni.
- **CEO** : promuove la cultura della sicurezza delle informazioni e assicura l'allineamento tra gli obiettivi di sicurezza e gli indirizzi strategici aziendali.
- **PRRC - Risk Manager Cyber & IT** : gestisce il SGSI, supervisiona i controlli tecnici e organizzativi di sicurezza e coordina la risposta agli incidenti.
- **Responsabile del Sistema Integrato (RSI)** : assicura il coordinamento trasversale tra il SGSI e le altre componenti del SGI, garantendo la coerenza complessiva delle politiche e dei processi.
- **QA - Enterprise & Quality Risk Manager** : integra la valutazione dei rischi di sicurezza delle informazioni nel processo complessivo di gestione dei rischi aziendali.
- **DPO / RPD (GDPR)** : verifica la conformità dei trattamenti di dati personali alla normativa sulla protezione dei dati e fornisce consulenza su impatti e rischi connessi alla privacy.
- **Responsabile Formazione e Qualifica Operatori** : pianifica e supervisiona i programmi di formazione e sensibilizzazione del personale in materia di sicurezza delle informazioni.
- **Tutto il personale** : osserva le politiche, le procedure e le istruzioni operative di sicurezza delle informazioni, segnalando tempestivamente qualsiasi evento sospetto o anomalia.

Obiettivi di sicurezza delle informazioni

L'organizzazione persegue obiettivi di sicurezza delle informazioni coerenti con il proprio contesto operativo di sanità digitale e telemedicina, con i rischi identificati e con gli indirizzi strategici definiti dal Top Management. Tali obiettivi, misurabili attraverso indicatori di prestazione verificati almeno annualmente in sede di riesame della direzione, si articolano nelle seguenti direttrici:

- protezione della riservatezza, dell'integrità e della disponibilità dei dati sanitari, personali e aziendali trattati attraverso la piattaforma Dr.Feel e le infrastrutture cloud dell'organizzazione;
- riduzione dell'esposizione ai rischi di sicurezza delle informazioni entro le soglie di tolleranza definite nel processo di valutazione dei rischi, con particolare attenzione ai rischi di accesso non autorizzato ai sistemi, uso insufficiente della crittografia e carenza di governance IT;
- mantenimento della conformità ai requisiti legali, normativi e contrattuali applicabili, tra cui il Reg. (UE) 2016/679 e la ISO/IEC 27001:2022;
- rafforzamento della consapevolezza e delle competenze del personale in materia di sicurezza delle informazioni, mediante programmi di formazione e sensibilizzazione periodici;
- miglioramento continuo dell'efficacia del SGSI attraverso audit interni, analisi degli incidenti, revisione dei rischi e riesame della direzione.

L'organizzazione si impegna a documentare ciascun obiettivo nella pianificazione del SGI, associandovi tempi, risorse, responsabilità e criteri di verifica dell'efficacia, secondo le modalità stabilite nella *PRO Obiettivi e pianificazione per il loro raggiungimento* .

Principi fondamentali di sicurezza delle informazioni

Approccio basato sul rischio

L'organizzazione fonda ogni decisione in materia di sicurezza delle informazioni sulla valutazione sistematica dei rischi e delle opportunità. I rischi vengono identificati, analizzati e trattati secondo la metodologia definita nella *PRO Procedura di gestione dei rischi* , che prevede la determinazione della probabilità e dell'impatto di ciascun evento, la definizione di una soglia di tolleranza e l'adozione di misure di mitigazione proporzionate. Il Top Management riesamina periodicamente il profilo di rischio dell'organizzazione per assicurare che i controlli restino adeguati all'evoluzione delle minacce e del contesto operativo, con particolare attenzione ai rischi connessi alla gestione di dati sanitari in ambiente digitale e cloud.

Classificazione e protezione delle informazioni

Dr.Feel Srl adotta un sistema di classificazione delle informazioni articolato in tre livelli di criticità, al fine di garantire che le misure di protezione siano proporzionate alla sensibilità dei dati trattati:

- **Riservato** : informazioni altamente sensibili il cui accesso è strettamente limitato e integralmente tracciato; richiedono cifratura sia a riposo sia in transito e non possono

essere conservate su dispositivi personali o non autorizzati.

- **Limitato** : informazioni proprietarie dell'organizzazione accessibili esclusivamente in base al principio della necessità di conoscenza; costituiscono il livello predefinito per tutte le informazioni non altrimenti classificate.
- **Pubblico** : informazioni destinate alla diffusione esterna, prive di requisiti specifici di protezione.

La *POL Politica di classificazione ed etichettatura delle informazioni* dettaglia i criteri di etichettatura e i requisiti di trattamento, trasmissione e conservazione associati a ciascun livello.

Uso accettabile delle informazioni e delle risorse

L'organizzazione si impegna a definire e comunicare regole chiare per l'utilizzo corretto delle informazioni, dei sistemi e delle risorse aziendali. Ogni membro del personale utilizza gli asset assegnati esclusivamente per finalità lavorative, li custodisce con diligenza e segnala immediatamente lo smarrimento, il furto o il danneggiamento di qualsiasi bene aziendale. L'assegnazione e la restituzione dei beni sono formalizzate tramite il *MOD Modulo di assegnazione dei beni* , mentre gli utenti autorizzati e i relativi diritti di accesso risultano documentati nel *Registro degli utenti autorizzati all'uso delle informazioni* . Le regole operative di dettaglio per l'uso accettabile sono contenute nella *POL Politica di sicurezza operativa* e nel *Codice di condotta* , la cui osservanza è vincolante per tutto il personale e i cui comportamenti inaccettabili, quali la condivisione di credenziali, il tentativo di elusione dei controlli di sicurezza e l'utilizzo di software non autorizzato, costituiscono violazioni gravi soggette a provvedimenti disciplinari.

Scrivania e schermo puliti

L'organizzazione promuove l'adozione di comportamenti che impediscano l'esposizione non autorizzata di informazioni, tanto in formato digitale quanto su supporto cartaceo. I dispositivi aziendali sono configurati con il blocco automatico dello schermo dopo un breve periodo di inattività e richiedono l'autenticazione per lo sblocco, prevenendo così la visualizzazione di informazioni da parte di soggetti non autorizzati. Ogni postazione di lavoro, in sede e da remoto, viene mantenuta priva di documenti classificati come Riservato o Limitato quando non è presidiata. Le regole applicative sono definite nella *POL Politica di sicurezza operativa* .

Segnalazione degli eventi di sicurezza delle informazioni

L'organizzazione mette a disposizione di tutto il personale un meccanismo tempestivo e accessibile per segnalare eventi di sicurezza delle informazioni osservati o sospetti, inclusi tentativi di phishing, comportamenti anomali dei sistemi e potenziali violazioni delle politiche. Le segnalazioni vengono indirizzate al **Chief Technology Officer** tramite il canale di comunicazione designato e registrate nel *MOD Registro degli incidenti di sicurezza delle informazioni* entro ventiquattro ore dalla rilevazione. L'intero ciclo di gestione dell'incidente, dalla classificazione iniziale fino

all'analisi post-incidente, è disciplinato dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Responsabilità condivisa

La sicurezza delle informazioni non ricade esclusivamente su una singola funzione aziendale, ma costituisce un impegno di ogni persona che interagisce con il patrimonio informativo dell'organizzazione. Il Top Management promuove una cultura diffusa di attenzione alla sicurezza, sostenuta da programmi periodici di formazione e sensibilizzazione, affinché ciascun ruolo sia consapevole dei rischi connessi alle proprie attività e agisca in coerenza con le politiche e le procedure del SGSI. La *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* formalizza le attribuzioni specifiche di ciascuna funzione.

Conformità normativa e miglioramento continuo

L'organizzazione si impegna a soddisfare i requisiti legali, normativi e contrattuali applicabili in materia di sicurezza delle informazioni e di protezione dei dati personali. Il SGSI è sottoposto a un ciclo continuo di verifica e miglioramento, alimentato dagli esiti degli audit interni, dall'analisi degli incidenti, dalla revisione dei rischi e dal riesame della direzione, al fine di garantire che i controlli adottati restino efficaci e proporzionati al contesto di minaccia in evoluzione.

Protezione degli asset fuori sede

L'organizzazione riconosce che la crescente diffusione del lavoro da remoto e della mobilità professionale espone gli asset informativi a rischi aggiuntivi al di fuori del perimetro fisico della sede aziendale. Dr.Feel Srl adotta pertanto misure specifiche per tutelare la riservatezza, l'integrità e la disponibilità delle informazioni trattate tramite dispositivi utilizzati in smart working, trasferta o altre situazioni operative fuori sede. Rientrano in tale ambito, a titolo esemplificativo, notebook, smartphone e tablet assegnati al personale.

In materia di **custodia** , l'organizzazione richiede che i dispositivi aziendali non siano mai lasciati incustoditi in luoghi pubblici, veicoli o aree comuni di strutture ricettive e di coworking. In trasferta, i dispositivi sono conservati in ambienti sicuri e chiusi a chiave sotto la responsabilità del personale assegnatario. La postazione di lavoro da remoto è configurata in modo che l'accesso fisico sia limitato alle sole persone autorizzate, impedendo a soggetti terzi di visualizzare lo schermo o di accedere ai dispositivi.

Per quanto riguarda l' **utilizzo sicuro** , il personale che opera fuori sede impiega esclusivamente dispositivi autorizzati dall'organizzazione, si connette ai sistemi aziendali tramite VPN e utilizza reti domestiche protette con cifratura almeno WPA2, avendo cura di modificare le credenziali predefinite del router. L'uso di reti Wi-Fi pubbliche non protette per il trattamento di informazioni aziendali classificate come Riservato o Limitato non è consentito. Tutte le comunicazioni che coinvolgono informazioni riservate avvengono unicamente attraverso i canali approvati dall'organizzazione; l'impiego di applicazioni di messaggistica personale e di account di posta non aziendali per la trasmissione di dati classificati è vietato.

In relazione alla **segnalazione di smarrimento, furto o danneggiamento** , il personale notifica immediatamente al **Chief Technology Officer** qualsiasi evento che comprometta un asset aziendale fuori sede, e in ogni caso non oltre ventiquattro ore dall'accadimento. La segnalazione attiva le misure di blocco remoto del dispositivo, revoca degli accessi e sostituzione delle credenziali compromesse. L'evento è trattato come incidente di sicurezza delle informazioni secondo quanto previsto dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Quanto alla **restituzione** , al termine del rapporto di lavoro, della trasferta o del progetto, ogni asset aziendale è restituito integro all'organizzazione, al netto della normale usura. La restituzione è formalizzata attraverso il *MOD Modulo di assegnazione dei beni* , che ne documenta lo stato al momento del rientro.

Archiviazione e aggiornamento

La presente politica è un documento controllato del Sistema di Gestione Integrato (SGI). Viene riesaminata con cadenza almeno annuale, ovvero in occasione di cambiamenti significativi nel contesto organizzativo, tecnologico o normativo, o a seguito di incidenti di sicurezza rilevanti. Il **Responsabile del Sistema Integrato (RSI)** , in collaborazione con il **Chief Technology Officer - PRRC - Risk Manager Cyber & IT** , coordina il processo di revisione e aggiornamento. Ogni nuova versione è sottoposta all'approvazione della **Direzione** prima della distribuzione a tutto il personale interessato e alle parti interessate rilevanti.

Documenti di riferimento

- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Obiettivi e pianificazione per il loro raggiungimento
- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni
- Codice di condotta
- MOD Modulo di assegnazione dei beni
- Registro degli utenti autorizzati all'uso delle informazioni
- MOD Registro degli incidenti di sicurezza delle informazioni