Pubblico

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	11/02/2026	Giacomo Manca	Iessica Gianello

Indice

Scopo

La presente politica rappresenta il documento cardine del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) di DOCUMENTAPLM.IT S.r.l. e formalizza l'impegno del Top Management verso la protezione degli asset informativi dell'organizzazione. Con essa, la direzione stabilisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il SGSI, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni trattate nell'ambito della progettazione, dello sviluppo, della gestione e della commercializzazione delle applicazioni software proprietarie.

DOCUMENTAPLM.IT S.r.l. riconosce che la sicurezza delle informazioni costituisce un fattore abilitante per la credibilità sul mercato B2B e per la continuità del proprio business. L'organizzazione promuove pertanto una cultura della sicurezza diffusa a tutto il personale, fondata su un approccio basato sul rischio e sulla responsabilità condivisa, in modo che ogni decisione operativa e strategica tenga conto delle esigenze di protezione dei dati e dei sistemi. La politica si propone inoltre di assicurare la conformità ai requisiti normativi e contrattuali applicabili, sostenendo gli indirizzi strategici della direzione e alimentando la fiducia dei clienti manifatturieri che affidano i propri processi alle soluzioni dell'organizzazione.

Campo di applicazione

La presente politica si applica a tutte le attività connesse alla progettazione, sviluppo, gestione e commercializzazione delle applicazioni software proprietarie di DOCUMENTAPLM.IT S.r.l., erogate secondo il modello di licenza on-premise. Coinvolge tutto il personale dell'organizzazione — amministratori, quadri, sviluppatori e tecnici applicativi — nonché i collaboratori esterni e le terze parti che accedono alle informazioni o ai sistemi aziendali. Il perimetro comprende tutti gli asset informativi, i repository documentali, i sistemi di sviluppo e gli strumenti di comunicazione utilizzati nell'operatività quotidiana, indipendentemente dalla collocazione fisica del personale. Sono esclusi dal campo di applicazione i processi relativi alla gestione di sedi fisiche proprie, in coerenza con l'assetto logistico dell'organizzazione che non detiene né gestisce un sito operativo in proprietà.

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.

- **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.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo per modificare il rischio.
- **Evento di sicurezza delle informazioni** : occorrenza identificata relativa a un sistema, servizio o rete, che indica una possibile violazione della politica di sicurezza delle informazioni o un fallimento dei controlli.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni indesiderati o inattesi che hanno una significativa probabilità 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, compresi processi, politiche, dispositivi, pratiche o altre condizioni e/o azioni.
- **Politica** : intenzioni e direzione di un'organizzazione come espresse formalmente dal suo Top Management.

Ruoli e responsabilità

- **Amministratore A** : approva la presente politica e le risorse necessarie al SGSI, assumendo la responsabilità ultima della direzione strategica in materia di sicurezza delle informazioni.
- **Amministratore B** : garantisce che le scelte di architettura e sviluppo tecnico siano coerenti con i principi di sicurezza definiti nella presente politica.
- **Responsabile del sistema di gestione** : coordina l'attuazione, il monitoraggio e il miglioramento continuo del SGSI, assicurando che la politica sia comunicata, compresa e applicata nell'intera organizzazione.
- **Quadro commerciale** : assicura che gli impegni di sicurezza delle informazioni siano rispettati nelle relazioni con i clienti e nelle attività commerciali.
- **Quadro sviluppatore** : verifica che le pratiche di sviluppo software rispettino i requisiti di protezione degli asset informativi stabiliti dalla presente politica.
- **Sviluppatore** : applica i principi di sicurezza delle informazioni nelle attività quotidiane di codifica, test e manutenzione del software.
- **Tecnico applicativo** : tutela le informazioni dei clienti durante le attività di configurazione, supporto tecnico e formazione.

Obiettivi di sicurezza delle informazioni

DOCUMENTAPLM.IT S.r.l. persegue obiettivi di sicurezza delle informazioni misurabili e coerenti con la propria strategia aziendale. Tali obiettivi sono riesaminati periodicamente dalla direzione e declinati nelle seguenti aree:

- **Protezione degli asset informativi** : mantenere un livello di rischio residuo entro la soglia di accettabilità definita nel processo di valutazione dei rischi, agendo tempestivamente quando il livello supera il valore di tolleranza stabilito.
- **Conformità normativa e contrattuale** : assicurare il pieno rispetto dei requisiti derivanti dalla legislazione vigente, dagli standard di riferimento e dagli obblighi contrattuali verso i clienti.
- **Continuità del servizio** : preservare la disponibilità dei sistemi e delle informazioni necessarie allo sviluppo, alla manutenzione e alla commercializzazione delle applicazioni software proprietarie.
- **Consapevolezza e competenza** : promuovere un livello di consapevolezza adeguato in tutto il personale, affinché ciascuno conosca le proprie responsabilità e contribuisca attivamente alla protezione delle informazioni.
- **Miglioramento continuo** : alimentare il ciclo di miglioramento del SGSI attraverso il monitoraggio degli indicatori, l'analisi delle non conformità e la definizione di azioni correttive efficaci.

Questi obiettivi sono tradotti in indicatori specifici, monitorati dal **Responsabile del sistema di gestione** e riesaminati in sede di riesame della direzione.

Principi fondamentali di sicurezza delle informazioni

L'organizzazione fonda il proprio SGSI sui principi che seguono, i quali orientano tutte le politiche specifiche, le procedure e i comportamenti individuali in materia di sicurezza.

Approccio basato sul rischio. Ogni decisione relativa alla sicurezza delle informazioni è sostenuta da una valutazione strutturata dei rischi, condotta secondo la metodologia definita nella *PRO Procedura di gestione dei rischi* . L'organizzazione identifica le minacce e le vulnerabilità rilevanti, ne stima la probabilità e l'impatto e stabilisce le contromisure proporzionate al livello di rischio risultante, intervenendo prioritariamente quando il punteggio supera la soglia di tolleranza.

Classificazione e protezione proporzionata delle informazioni. Tutte le informazioni gestite dall'organizzazione sono classificate secondo tre livelli — riservato, limitato e pubblico — e protette con misure adeguate alla rispettiva sensibilità, come dettagliato nella *POL Politica di classificazione ed etichettatura delle informazioni* . L'assegnazione di diritti di accesso avviene esclusivamente in base alla necessità operativa dimostrata e al principio del minimo privilegio.

Uso accettabile delle informazioni e degli asset associati. L'organizzazione stabilisce regole esplicite per l'impiego corretto delle informazioni e delle risorse a esse connesse, documentate nella *POL Politica di sicurezza operativa* e nel *Registro degli utenti autorizzati all'uso delle informazioni* . L'assegnazione formale degli asset al personale avviene tramite

il *MOD Modulo di assegnazione dei beni* ; ogni assegnatario è responsabile dell'uso conforme e della restituzione al termine del rapporto o dell'esigenza operativa.

Scrivania pulita e schermo pulito. L'organizzazione adotta regole di scrivania pulita e schermo pulito per prevenire l'accesso non autorizzato alle informazioni. I dispositivi aziendali sono configurati con il blocco automatico dello schermo dopo un periodo di inattività e ogni membro del personale è tenuto a non lasciare documenti o supporti contenenti informazioni sensibili esposti in aree accessibili, sia in sede sia durante il lavoro da remoto. Le regole operative specifiche sono definite nella *POL Politica di sicurezza operativa* .

Segnalazione tempestiva degli eventi di sicurezza. L'organizzazione predispone un canale dedicato attraverso cui tutto il personale — inclusi collaboratori e terze parti — segnala tempestivamente ogni evento di sicurezza delle informazioni osservato o sospetto, come dettagliato nella *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* . L'organizzazione si impegna a non sanzionare le segnalazioni effettuate in buona fede e a trattare ogni segnalazione con la massima riservatezza.

Responsabilità condivisa. La sicurezza delle informazioni non è competenza esclusiva di una singola funzione: ciascun membro del personale contribuisce alla protezione degli asset informativi nel rispetto dei propri compiti, come formalizzato nella *POL Politica dei ruoli e delle responsabilità in materia di sicurezza delle informazioni* e nel *Codice di condotta* . Il Top Management sostiene questa cultura attraverso l'allocazione delle risorse necessarie e la verifica periodica dell'efficacia dei controlli.

Conformità e miglioramento continuo. L'organizzazione si impegna a soddisfare i requisiti legali, regolamentari e contrattuali applicabili, a monitorare l'efficacia del SGSI mediante audit interni e indicatori di prestazione e a perseguire il miglioramento continuo attraverso la correzione delle non conformità e l'individuazione sistematica di opportunità di rafforzamento.

Protezione degli asset fuori sede

DOCUMENTAPLM.IT S.r.l. riconosce che una parte significativa delle proprie attività si svolge al di fuori di una sede fisica tradizionale e si impegna a garantire lo stesso livello di protezione degli asset informativi indipendentemente dalla loro collocazione. Questa sezione enuncia i principi che guidano la tutela dei dispositivi, dei supporti e delle informazioni utilizzati in contesti di lavoro da remoto, trasferta o prestito d'uso.

Conformità dei dispositivi remoti. I notebook e le altre risorse informatiche utilizzati per accedere ai sistemi aziendali da qualsiasi luogo esterno devono rispettare i requisiti di sicurezza stabiliti dalla presente politica e dalle politiche operative correlate. Il personale è tenuto a mantenere attivi e aggiornati i controlli di sicurezza presenti sul dispositivo — software antivirus, firewall personale — e a non modificare né disattivare le configurazioni predisposte dall'organizzazione.

Protezione delle connessioni di rete. L'accesso ai sistemi interni da postazioni remote avviene esclusivamente attraverso la VPN aziendale. L'utilizzo di reti Wi-Fi pubbliche con dispositivi aziendali è vietato; quando ci si collega a una rete domestica, le credenziali di amministrazione del router devono essere state personalizzate rispetto ai valori predefiniti dal produttore.

Custodia e trasporto. Il personale non lascia i dispositivi aziendali incustoditi in luoghi pubblici, mezzi di trasporto o aree comuni di strutture condivise. In caso di trasferta, i dispositivi sono conservati in luogo protetto sotto la responsabilità dell'assegnatario. L'uscita dei dispositivi dall'organizzazione è formalizzata tramite il *MOD Modulo di assegnazione dei beni* , che riporta il modello del dispositivo, il numero di serie e i dati dell'assegnatario.

Comportamento dell'operatore. Durante il lavoro da remoto si applicano integralmente le regole di scrivania pulita, di gestione della stampa e di smaltimento sicuro delle risorse, così come l'obbligo di segnalare tempestivamente qualsiasi evento di sicurezza delle informazioni attraverso il canale dedicato. L'area di lavoro deve essere organizzata in modo tale da impedire la visione dello schermo e dei documenti da parte di persone non autorizzate.

Segnalazione di smarrimento, furto o danneggiamento. Il personale notifica immediatamente al **Responsabile del sistema di gestione** qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le misure di blocco remoto del dispositivo, la revoca degli accessi e il cambio delle credenziali associate. L'evento è trattato come evento di sicurezza delle informazioni ai sensi della *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Restituzione. Al termine del rapporto di lavoro, della collaborazione, del progetto o del periodo di lavoro da remoto, l'asset è restituito all'organizzazione nella medesima modalità documentale con cui è stato assegnato.

Archiviazione e aggiornamento

La presente politica è gestita come informazione documentata del SGSI ai sensi della *PRO Procedura di gestione delle informazioni documentate* . Il **Responsabile del sistema di gestione** ne assicura la conservazione nella versione vigente all'interno del sistema documentale aziendale e la rende accessibile a tutto il personale interessato. La politica è riesaminata almeno una volta all'anno e ogni qualvolta intervengano cambiamenti significativi nel contesto organizzativo, nelle minacce, nella tecnologia o nei requisiti normativi applicabili. Le modifiche sono approvate dall' **Amministratore A** e comunicate a tutto il personale e alle parti interessate pertinenti.

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 dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di gestione delle informazioni documentate
- PRO Procedura di configurazione, gestione e smaltimento degli asset

- Codice di condotta
- Registro degli utenti autorizzati all'uso delle informazioni
- MOD Modulo di assegnazione dei beni