Pubblico

POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	06/04/2026	Fedrico Diego Merello	Nicola Lonato

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 esprime la volontà del **Top Management** di WIP Italia S.r.l. di proteggere il patrimonio informativo aziendale e rappresenta il documento di indirizzo al vertice del Sistema di Gestione Integrato (SGI) per quanto concerne la sicurezza delle informazioni. Attraverso questo documento l'organizzazione definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare nel tempo le misure a presidio della riservatezza, dell'integrità e della disponibilità delle informazioni, in coerenza con gli obiettivi strategici aziendali.

WIP Italia riconosce che la sicurezza delle informazioni costituisce un fattore abilitante per il proprio business di progettazione, sviluppo e manutenzione di soluzioni e prodotti digitali, siti web, piattaforme e-commerce e applicazioni web e mobile. L'Alta Direzione promuove una cultura della sicurezza fondata sulla consapevolezza, sulla responsabilità condivisa e sull'allocazione delle risorse necessarie, assicurando che i requisiti del SGI trovino piena integrazione nei processi aziendali e che la loro efficacia sia verificata attraverso attività di riesame periodiche.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di WIP Italia S.r.l. presso la sede operativa di Viale Monza 1, 20125 Milano, compresi i sistemi tecnologici e le infrastrutture utilizzate per l'erogazione dei servizi di consulenza, digital strategy, experience design, sviluppo software e system integration. Coinvolge tutto il personale dipendente, i collaboratori a contratto e le terze parti autorizzate ad accedere alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro adottata, incluso il lavoro da remoto. Sono esclusi dall'ambito di applicazione i sistemi e i dati gestiti interamente e autonomamente dai clienti, salvo diverso accordo contrattuale.

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 di un'entità autorizzata.
- **Rischio** : effetto dell'incertezza sugli obiettivi, espresso in termini di combinazione della probabilità di un evento e delle sue conseguenze.
- **Valutazione del rischio** : processo complessivo di identificazione, analisi e ponderazione del rischio.
- **Trattamento del rischio** : processo finalizzato a modificare il rischio attraverso la selezione e l'attuazione di misure appropriate.
- **Asset informativo** : qualsiasi elemento di valore per l'organizzazione che contribuisce all'elaborazione, alla conservazione o alla trasmissione delle informazioni.
- **Controllo** : misura tecnica, organizzativa, gestionale o legale che modifica il rischio.
- **Parte interessata** : persona o organizzazione che può influire su una decisione o un'attività dell'organizzazione, esserne influenzata o percepirsi come tale.
- **Miglioramento continuo** : attività ricorrente finalizzata ad accrescere le prestazioni del sistema di gestione.
- **Dato personale** : qualsiasi informazione riguardante una persona fisica identificata o identificabile.

Ruoli e responsabilità

- Il **Top Management** approva la presente politica, ne garantisce la coerenza con l'indirizzo strategico dell'organizzazione e assicura la disponibilità delle risorse necessarie alla sua attuazione.
- Il **Responsabile del Sistema di Gestione** supervisiona l'attuazione, il monitoraggio e il riesame delle misure di sicurezza delle informazioni previste dal SGI, curandone la comunicazione a tutto il personale e coordinando le attività di audit e miglioramento.
- Il personale, i collaboratori e le terze parti autorizzate rispettano le disposizioni della presente politica e delle politiche e procedure collegate, segnalando tempestivamente qualunque evento o vulnerabilità di sicurezza attraverso i canali predisposti dall'organizzazione.

Obiettivi di sicurezza delle informazioni

WIP Italia persegue obiettivi di sicurezza delle informazioni allineati al proprio indirizzo strategico e al contesto in cui opera, garantendone la comunicazione, la misurabilità e la revisione periodica in sede di riesame della direzione. L'organizzazione si propone di:

- Salvaguardare la riservatezza, l'integrità e la disponibilità delle informazioni aziendali e dei clienti lungo l'intero ciclo di vita dei progetti, dalla consulenza strategica alla manutenzione delle soluzioni digitali rilasciate.
- Assicurare la conformità ai requisiti normativi e contrattuali applicabili, con particolare riguardo alla protezione dei dati personali e alla sicurezza delle informazioni.

- Contenere l'esposizione ai rischi di sicurezza delle informazioni mediante l'adozione sistematica di un approccio basato sul rischio, selezionando e dimensionando le misure di mitigazione in funzione della probabilità e dell'impatto degli scenari individuati.
- Rafforzare la consapevolezza e la competenza del personale in materia di sicurezza attraverso programmi di formazione e sensibilizzazione ricorrenti, affinché ciascun collaboratore riconosca il proprio ruolo nella protezione del patrimonio informativo.
- Garantire la continuità operativa dei servizi erogati ai clienti, minimizzando gli effetti di incidenti, interruzioni e situazioni di emergenza sui processi critici.
- Consolidare la fiducia di clienti e parti interessate attraverso una governance trasparente della sicurezza e il miglioramento costante dei controlli adottati.

Principi fondamentali di sicurezza delle informazioni

WIP Italia fonda la propria strategia di sicurezza su un insieme di principi che guidano ogni decisione e comportamento all'interno dell'organizzazione e che permeano l'intero corpo documentale del SGI. Tali principi si applicano a tutte le forme di informazione gestite dall'organizzazione, siano esse digitali, cartacee o verbali.

L'organizzazione adotta un approccio sistematico alla gestione del rischio che prevede l'identificazione, la valutazione e il trattamento dei rischi per la sicurezza delle informazioni in funzione della loro probabilità e del loro impatto. Le misure di protezione sono selezionate e dimensionate in modo proporzionato ai rischi individuati, tenendo conto del contesto operativo, delle esigenze dei clienti e dell'evoluzione del panorama delle minacce. La *PRO Procedura di gestione dei rischi* definisce la metodologia, le responsabilità e le soglie di tolleranza adottate, e i risultati delle valutazioni alimentano le scelte di investimento e il perfezionamento dei controlli.

Ogni informazione è classificata in base alla propria sensibilità, ai requisiti legali applicabili e alla criticità per il business, secondo i livelli stabiliti dalla *POL Politica di classificazione ed etichettatura delle informazioni* . L'organizzazione definisce e comunica regole per l'uso accettabile delle informazioni e delle risorse associate, affinché il personale gestisca gli asset informativi con consapevolezza e nel rispetto delle esigenze di protezione. L'assegnazione formale dei beni aziendali è tracciata nel *MOD Modulo di assegnazione dei beni* , mentre gli utenti autorizzati e i relativi ambiti di accesso sono documentati nel *Registro degli utenti autorizzati all'uso delle informazioni* .

WIP Italia promuove pratiche di scrivania pulita e schermo protetto per prevenire l'accesso non autorizzato e la divulgazione involontaria di informazioni riservate. I dispositivi aziendali sono dotati di meccanismi di blocco automatico dello schermo dopo un breve periodo di inattività, e i documenti cartacei contenenti informazioni classificate vengono custoditi in modo sicuro al termine della giornata lavorativa. La *POL Politica di sicurezza operativa* dettaglia i requisiti specifici applicabili a ciascun contesto di lavoro, incluse le postazioni remote.

L'organizzazione mette a disposizione di tutto il personale, dei collaboratori e delle terze parti un canale dedicato per segnalare tempestivamente qualsiasi evento di sicurezza osservato o sospetto, che si tratti di tentativi di phishing, anomalie nei sistemi, accessi non autorizzati o qualunque altra circostanza potenzialmente lesiva per il patrimonio informativo. Le segnalazioni sono indirizzate al **Responsabile del Sistema di Gestione** e

gestite secondo le fasi previste dalla *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* ; ogni evento è registrato nel *MOD Registro degli incidenti di sicurezza delle informazioni* ai fini di tracciabilità, analisi delle cause e apprendimento organizzativo.

In qualità di titolare del trattamento, WIP Italia si impegna a trattare i dati personali nel rispetto dei principi fondamentali sanciti dalla normativa europea, adottando misure tecniche e organizzative adeguate alla natura, all'ambito e alle finalità dei trattamenti effettuati. L'organizzazione persegue in particolare:

- La liceità, correttezza e trasparenza di ogni trattamento, fondato su una base giuridica documentata e comunicato agli interessati in modo chiaro e accessibile.
- La limitazione delle finalità e la minimizzazione dei dati raccolti, che restano adeguati, pertinenti e circoscritti a quanto strettamente necessario.
- L'esattezza delle informazioni e il loro tempestivo aggiornamento o rettifica.
- La limitazione della conservazione al periodo necessario al conseguimento delle finalità dichiarate.
- L'integrità e la riservatezza dei dati personali, tutelate mediante misure di sicurezza commisurate al rischio.

L'organizzazione pone il principio di responsabilizzazione alla base della propria governance dei dati personali: documenta le scelte effettuate, mantiene aggiornato il *MOD Registro dei trattamenti del titolare* , inventaria le misure tecniche e organizzative nel *MOD Elenco delle misure di sicurezza* e attesta formalmente il proprio impegno nella *MOD Dichiarazione di responsabilizzazione* . La *POL Politica del sistema privacy* traduce questi impegni in regole operative per l'intero ciclo di vita del dato.

La sicurezza delle informazioni resta una responsabilità che coinvolge ogni persona operante per conto dell'organizzazione. WIP Italia investe nella formazione e nella sensibilizzazione affinché ciascun collaboratore comprenda l'importanza del proprio contributo alla protezione del patrimonio informativo, agisca in conformità alle politiche adottate e partecipi attivamente al percorso di evoluzione del SGI.

Protezione degli asset fuori sede

WIP Italia si impegna a garantire un livello di protezione adeguato per gli asset informativi anche quando questi vengono utilizzati al di fuori della sede aziendale, in contesti quali il lavoro da remoto, le trasferte e le attività svolte presso sedi di clienti o partner. Rientrano fra gli asset fuori sede, a titolo esemplificativo, notebook e dispositivi mobili aziendali, supporti di memorizzazione rimovibili e documenti cartacei contenenti informazioni classificate.

La protezione di tali asset si fonda sui principi seguenti:

- **Custodia e sicurezza fisica** : il personale assegnatario custodisce i dispositivi aziendali con la diligenza richiesta dalla loro classificazione, evitando di lasciarli incustoditi in luoghi pubblici, veicoli o spazi condivisi. Gli schermi vengono posizionati in modo da impedire la visione delle informazioni da parte di soggetti non autorizzati, e il blocco automatico dello schermo resta attivo in ogni contesto operativo.

- **Accesso sicuro e cifratura** : l'accesso ai sistemi aziendali da postazioni remote avviene esclusivamente tramite connessione VPN e reti protette da cifratura adeguata. I dispositivi aziendali sono dotati di cifratura dell'intero disco e l'organizzazione adotta misure per consentire la cancellazione dei dati aziendali in caso di smarrimento o furto, a presidio della riservatezza delle informazioni.
- **Uso esclusivo e restrizioni** : i dispositivi forniti dall'organizzazione sono destinati esclusivamente alle attività lavorative aziendali e non possono essere ceduti o utilizzati da soggetti terzi. L'attività lavorativa da remoto è consentita unicamente presso il domicilio del collaboratore, un altro luogo privato o un hub aziendale; è espressamente vietato operare da luoghi pubblici o accessibili al pubblico.
- **Segnalazione di smarrimento, furto o danneggiamento** : qualunque evento di smarrimento, furto o danneggiamento di un asset aziendale fuori sede viene comunicato senza indugio al **Responsabile del Sistema di Gestione** mediante il canale di segnalazione dedicato. La segnalazione attiva le misure di contenimento, tra cui il blocco remoto del dispositivo e la revoca delle credenziali di accesso, e l'evento viene gestito come incidente di sicurezza delle informazioni secondo la *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .
- **Restituzione degli asset** : al termine della trasferta, del progetto o del rapporto di lavoro, ogni asset è restituito all'organizzazione. L'assegnazione degli asset è formalizzata nel *MOD Modulo di assegnazione dei beni* .

La *POL Politica di sicurezza operativa* dettaglia i requisiti tecnici e organizzativi applicabili al lavoro da remoto, alla protezione delle postazioni domestiche e alla sicurezza delle reti utilizzate dal personale al di fuori della sede aziendale.

Archiviazione e aggiornamento

La presente politica è un documento controllato del SGI, archiviato e reso accessibile a tutto il personale attraverso i canali di comunicazione interni dell'organizzazione. Il **Responsabile del Sistema di Gestione** ne cura il riesame con cadenza almeno annuale, ovvero in occasione di cambiamenti significativi nel contesto organizzativo, nel panorama normativo, nella tecnologia o nel quadro delle minacce alla sicurezza delle informazioni. Ogni revisione è sottoposta all'approvazione del **Top Management** prima della pubblicazione.

Documenti di riferimento

- POL Politica di classificazione ed etichettatura delle informazioni
- POL Politica di sicurezza operativa
- POL Politica del sistema privacy
- PRO Procedura di gestione dei rischi
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- MOD Modulo di assegnazione dei beni

- Registro degli utenti autorizzati all'uso delle informazioni
- MOD Registro degli incidenti di sicurezza delle informazioni
- MOD Elenco delle misure di sicurezza
- MOD Registro dei trattamenti del titolare
- MOD Dichiarazione di responsabilizzazione