POL Politica di sicurezza delle informazioni

Storia della versione

Versione	Data	Autore	Approvato da
1	22/04/2025	Fabio Damiani	Giuseppe Favilli
2	05/11/2025	Fabio Damiani	Giuseppe Favilli
3	01/09/2026	Fabio Damiani	Giuseppe Favilli

Indice

- Descrizione della versione
- 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

Descrizione della versione

Rispetto alla versione precedente, le principali modifiche sono:

- La sezione relativa alla protezione degli asset fuori sede è stata ampliata e resa autonoma, con l'introduzione di principi espliciti in materia di custodia, trasporto, segnalazione di smarrimento, furto o danneggiamento e restituzione dei beni aziendali.
- I contenuti riguardanti la struttura delle politiche, l'uso accettabile delle risorse, la segnalazione degli eventi di sicurezza e la sicurezza dell'ambiente di lavoro sono stati consolidati all'interno della sezione sui principi fondamentali, eliminando le sottosezioni separate presenti nella versione precedente.
- I ruoli e le responsabilità sono stati aggiornati per riflettere la struttura organizzativa corrente di Partech.

Scopo

Lo scopo della presente politica è dichiarare e comunicare l'impegno del Top Management di Partech verso la protezione degli asset informativi dell'organizzazione. Questo documento definisce il quadro di riferimento per istituire, attuare, mantenere e migliorare continuamente il Sistema di Gestione della Sicurezza delle Informazioni (SGSI), al fine di proteggere la riservatezza, l'integrità e la disponibilità delle informazioni e di supportare gli obiettivi strategici aziendali nel contesto dei servizi di consulenza progettuale, gestionale, di infrastrutture e sistemi e di informatica forense erogati da Partech.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi, gli asset informativi e i sistemi tecnologici gestiti da Partech presso la sede operativa di Largo A. Cacciari 1/b, 43122 Parma. Coinvolge tutto il personale, inclusi dipendenti, collaboratori a contratto e terze parti che hanno accesso alle informazioni o ai sistemi aziendali, indipendentemente dalla modalità di lavoro — in sede o da remoto.

Riferimenti normativi

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

Termini e definizioni

- **Riservatezza** : proprietà per cui le informazioni non sono rese disponibili o divulgate a individui, entità o processi non autorizzati.
- **Integrità** : proprietà di salvaguardare l'accuratezza e la completezza degli asset informativi.

- **Disponibilità** : proprietà di essere accessibile e utilizzabile su richiesta da parte di un'entità autorizzata.
- **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 malfunzionamento dei controlli.
- **Incidente di sicurezza delle informazioni** : uno o più eventi di sicurezza delle informazioni che hanno una probabilità significativa di compromettere le operazioni aziendali e di minacciare la sicurezza delle informazioni.

Ruoli e responsabilità

- **CEO / Top Management** : approva la presente politica, assicura la disponibilità delle risorse necessarie per il SGSI e promuove la cultura della sicurezza delle informazioni a tutti i livelli dell'organizzazione.
- **Responsabile del sistema di gestione** : governa la documentazione del SGSI, monitora il raggiungimento degli obiettivi di sicurezza e coordina le attività di riesame e miglioramento continuo.
- **CTO** : sviluppa e mantiene le politiche specifiche di sicurezza, gestisce i rischi informatici, coordina la risposta agli incidenti e promuove la formazione e la consapevolezza del personale in materia di sicurezza.
- **Responsabile IT** : implementa e gestisce i controlli tecnici di sicurezza a protezione dell'infrastruttura e degli asset IT, in conformità con le politiche aziendali.
- **Responsabile H&R** : assicura che la presa visione delle politiche di sicurezza sia parte integrante del processo di inserimento e che il personale riceva un'adeguata formazione sulla protezione delle informazioni.
- **Responsabile Protezione Dati** : garantisce la conformità ai requisiti normativi in materia di protezione dei dati personali e supporta le valutazioni d'impatto sulla privacy.

Obiettivi di sicurezza delle informazioni

Partech persegue la protezione della riservatezza, dell'integrità e della disponibilità dei propri asset informativi e di quelli dei clienti. Gli obiettivi strategici del SGSI, approvati dal **CEO / Top Management** e monitorati dal **Responsabile del sistema di gestione** in collaborazione con il **CTO** , sono i seguenti:

- **Protezione dei dati dei clienti** — Garantire la massima riservatezza e integrità delle informazioni gestite nell'ambito dei servizi di consulenza progettuale, gestionale e di informatica forense, prevenendo accessi, modifiche o divulgazioni non autorizzate.
- **Garanzia della continuità operativa** — Assicurare la disponibilità dei sistemi e delle infrastrutture informatiche per supportare i processi aziendali critici e l'erogazione continua dei servizi ai clienti, come definito nella *PRO Procedura di continuità operativa e di ripristino di emergenza* .

- **Conformità normativa e contrattuale** — Rispettare tutte le leggi, i regolamenti e gli obblighi contrattuali applicabili in materia di sicurezza delle informazioni e protezione dei dati personali.
- **Gestione proattiva del rischio** — Adottare un approccio basato sul rischio per identificare, valutare e trattare le minacce alla sicurezza delle informazioni, come descritto nella *PRO Procedura di gestione dei rischi* .
- **Promozione della cultura della sicurezza** — Sviluppare e mantenere un'elevata consapevolezza della sicurezza a tutti i livelli dell'organizzazione attraverso programmi di formazione e comunicazione continui.

Il processo di definizione, pianificazione e riesame di tali obiettivi è dettagliato nella *PRO Obiettivi e pianificazione per il loro raggiungimento* .

Principi fondamentali di sicurezza delle informazioni

Partech adotta un insieme gerarchico e coerente di politiche per la sicurezza delle informazioni. La presente politica rappresenta il documento di vertice che stabilisce gli indirizzi strategici; da essa discendono politiche specifiche per argomento — tra cui la *POL Politica di sicurezza operativa* e la *POL Politica di classificazione ed etichettatura delle informazioni* — che forniscono direttive dettagliate per ambiti particolari. Il **CEO / Top Management** approva la presente politica, mentre il **CTO** sviluppa e mantiene le politiche specifiche con l'approvazione della Direzione. L'intero corpus documentale è riesaminato con cadenza almeno annuale e ogni qualvolta si verifichino cambiamenti significativi, secondo quanto stabilito nella *PRO Gestione riesame della direzione* .

Tutte le politiche di sicurezza delle informazioni sono comunicate a tutto il personale e, ove pertinente, alle parti esterne interessate. Il **Responsabile H&R** assicura che la presa visione delle politiche sia parte integrante del processo di inserimento di nuovo personale, promuovendo la piena consapevolezza dei comportamenti attesi.

Partech riconosce che la responsabilità in materia di sicurezza è condivisa e si estende a ogni persona che utilizza le risorse dell'organizzazione. L'azienda promuove pertanto i seguenti principi trasversali.

Uso accettabile delle risorse. Tutti gli asset informativi di Partech — hardware, software, dati e risorse di rete — sono destinati a un uso responsabile, etico e conforme agli scopi aziendali autorizzati. L'organizzazione definisce e aggiorna regole specifiche di utilizzo nella *POL Politica di sicurezza operativa* e nel *Codice di condotta* , la cui osservanza è obbligatoria per il personale e i collaboratori. L'assegnazione formale dei beni avviene tramite il *MOD Modulo di assegnazione dei beni* , che vincola l'assegnatario alla custodia responsabile.

Segnalazione degli eventi di sicurezza. Partech riconosce nella tempestività della segnalazione un fattore determinante per contenere le conseguenze di eventuali incidenti. Ogni membro del personale contribuisce attivamente alla protezione degli asset segnalando immediatamente qualsiasi evento, anomalia o debolezza di sicurezza — anche solo sospetta — attraverso i canali designati: comunicazione al proprio superiore gerarchico, posta elettronica dedicata al team di sicurezza o apertura di un ticket sul sistema di gestione interno. Il **CTO** coordina la ricezione e il trattamento di tali segnalazioni; ogni incidente è registrato nel *MOD Registro degli incidenti di sicurezza delle*

informazioni e trattato secondo la *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Sicurezza dell'ambiente di lavoro. Partech adotta misure volte a proteggere le informazioni da accessi non autorizzati, danni e interferenze, sia negli uffici aziendali sia in postazioni di lavoro remote. Le postazioni sono mantenute sgombre da documenti e supporti di memorizzazione contenenti informazioni sensibili al di fuori dell'orario di lavoro, in coerenza con la *POL Politica di classificazione ed etichettatura delle informazioni* . Tutti i dispositivi sono configurati per attivare un blocco schermo protetto da credenziali dopo un massimo di cinque minuti di inattività; il personale blocca manualmente la propria sessione ogni volta che si allontana dalla postazione. Il **Responsabile IT** è responsabile dell'implementazione tecnica di tali controlli.

Protezione degli asset fuori sede

Partech tutela i propri asset informativi anche quando il personale li utilizza al di fuori dei locali aziendali — in modalità di lavoro remoto, durante trasferte o presso sedi di clienti. L'organizzazione si impegna a garantire che i dispositivi portatili, i supporti fisici e i documenti trasportati al di fuori del perimetro aziendale mantengano un livello di protezione equivalente a quello assicurato in sede. A tal fine si applicano i seguenti principi.

Custodia. Gli asset aziendali non sono mai lasciati incustoditi in veicoli, mezzi pubblici, aree comuni di strutture ricettive o spazi di coworking. In trasferta, il personale assegnatario li custodisce nella cassaforte della struttura ospitante o in un luogo chiuso a chiave.

Trasporto. L'asset è trasportato in custodia personale. Per consegne a consulenti, fornitori o sedi distaccate si utilizza un servizio di corriere tracciato.

Segnalazione di smarrimento, furto o danneggiamento. Il personale notifica immediatamente al **Responsabile IT** qualunque smarrimento, furto o danneggiamento di asset aziendali fuori sede. La segnalazione attiva le procedure di blocco remoto del dispositivo, revoca degli accessi e cambio delle credenziali. L'evento è registrato come incidente di sicurezza delle informazioni secondo la *PRO Procedura di gestione degli incidenti di sicurezza delle informazioni* .

Lavoro remoto. Il personale che opera in modalità remota rispetta le disposizioni definite nell'accordo individuale di lavoro remoto e nelle regole aziendali di sicurezza. In particolare è fatto divieto di utilizzo di reti Wi-Fi pubbliche con i dispositivi aziendali; l'accesso alla rete aziendale avviene esclusivamente tramite gli strumenti di connessione sicura forniti dall'azienda, configurati con autenticazione a più fattori. I dipendenti non possono modificare o disattivare i controlli di sicurezza organizzativi sui sistemi utilizzati per accedere alle risorse aziendali.

Restituzione. Al termine della trasferta, del progetto o del rapporto di lavoro, l'asset è restituito all'organizzazione tramite il *MOD Modulo di assegnazione dei beni* . La gestione del ciclo di vita completo degli asset, incluso lo smaltimento sicuro, è disciplinata dalla *PRO Procedura di configurazione, gestione e smaltimento degli asset* .

Archiviazione e aggiornamento

Il presente documento è gestito in forma controllata e archiviato secondo le modalità definite nella *PRO Procedura di gestione delle informazioni documentate* . La politica è soggetta a revisione periodica con cadenza almeno annuale, o a seguito di cambiamenti significativi nel contesto aziendale, tecnologico o normativo, sotto la supervisione del **Responsabile del sistema di gestione** . Ogni aggiornamento è approvato dal **CEO / Top Management** e comunicato a tutto il personale.

Documenti di riferimento

- Codice di condotta
- MOD Modulo di assegnazione dei beni
- MOD Registro degli incidenti di sicurezza delle informazioni
- POL Politica di sicurezza operativa
- POL Politica di classificazione ed etichettatura delle informazioni
- PRO Procedura di continuità operativa e di ripristino di emergenza
- PRO Procedura di gestione dei rischi
- PRO Obiettivi e pianificazione per il loro raggiungimento
- PRO Gestione riesame della direzione
- PRO Procedura di gestione degli incidenti di sicurezza delle informazioni
- PRO Procedura di configurazione, gestione e smaltimento degli asset
- PRO Procedura di gestione delle informazioni documentate