

POL Politica del sistema di gestione

Storia della versione

Versione	Data	Autore	Approvato da
1	05/05/2026	Responsabile del sistema di gestione	Direzione

Indice

- Scopo
- Campo di applicazione
- Riferimenti normativi
- Termini e definizioni
- Ruoli e responsabilità
- Impegno e obiettivi del sistema di gestione
- Archiviazione e aggiornamento
- Documenti di riferimento

Scopo

Joinrs S.r.l. opera nel settore della tecnologia per le risorse umane, progettando, sviluppando e gestendo una piattaforma SaaS che connette talenti junior e neolaureati con opportunità professionali attraverso soluzioni di matching basate sull'intelligenza artificiale e servizi di employer branding. In questo contesto, la protezione delle informazioni rappresenta un pilastro strategico per la sostenibilità e la competitività dell'organizzazione.

La presente politica esprime la visione e gli impegni del Top Management in materia di sicurezza delle informazioni e, insieme alla *POL Politica di sicurezza delle informazioni*, costituisce il quadro documentale di riferimento del Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Il suo scopo è definire il quadro di riferimento entro cui l'organizzazione persegue la tutela della riservatezza, dell'integrità e della disponibilità degli asset informativi, in coerenza con il proprio contesto operativo, le esigenze delle parti interessate e gli indirizzi strategici aziendali.

Joinrs riconosce che la fiducia dei clienti corporate, dei candidati e dei partner istituzionali si fonda sulla capacità di garantire una gestione responsabile dei dati e dei sistemi. La politica intende pertanto promuovere una cultura diffusa della sicurezza, orientata al rispetto della normativa vigente e al miglioramento continuo delle pratiche di protezione delle informazioni, affinché ogni decisione aziendale tenga conto dei rischi e delle opportunità connessi alla sicurezza.

Campo di applicazione

La presente politica si applica a tutte le attività, i processi e gli asset informativi di Joinrs S.r.l. coinvolti nella progettazione, nello sviluppo, nell'erogazione e nella gestione della piattaforma SaaS Joinrs, delle soluzioni di matching basate sull'intelligenza artificiale e dei servizi di employer branding. Il suo perimetro comprende tutte le sedi dell'organizzazione: la sede legale di Roma (Via Marsala 29 H), l'ufficio operativo di Milano (Via San Francesco d'Assisi 15) e la sede di Madrid. Essa si rivolge a tutto il personale, inclusi dipendenti, collaboratori e terze parti che accedono ai sistemi o alle informazioni aziendali, indipendentemente dalla localizzazione geografica o dalla modalità di lavoro, compreso il lavoro da remoto. Sono esclusi dal campo di applicazione i servizi occasionali di selezione del personale e le attività di sviluppo eventualmente affidate a soggetti esterni, poiché l'intero sviluppo della piattaforma è gestito internamente.

Riferimenti normativi

- ISO/IEC 27001:2022
- Regolamento (UE) 2016/679
- D.Lgs. 196/2003
- Regolamento (UE) 2024/1689
- Direttiva (UE) 2022/2555

Termini e definizioni

- **Sicurezza delle informazioni** : preservazione della riservatezza, dell'integrità e della disponibilità delle informazioni.
- **Sistema di gestione della sicurezza delle informazioni (SGSI)** : parte del sistema di gestione complessivo, basata su un approccio al rischio, finalizzata a stabilire, implementare, operare, monitorare, riesaminare, mantenere e migliorare la sicurezza delle informazioni.
- **Politica** : intenzioni e direzione di un'organizzazione espresse formalmente dal suo Top Management.
- **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, attraverso la selezione e l'attuazione di opzioni che lo affrontino.
- **Parte interessata** : persona o organizzazione che può influenzare, essere influenzata da, o percepirsi influenzata da una decisione o attività.
- **Miglioramento continuo** : attività ricorrente svolta per accrescere le prestazioni.
- **Non conformità** : mancato soddisfacimento di un requisito.
- **Azione correttiva** : azione intrapresa per eliminare la causa di una non conformità e per prevenirne la ripetizione.
- **Informazioni documentate** : informazioni che devono essere controllate e mantenute da un'organizzazione e il supporto che le contiene.
- **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.

Ruoli e responsabilità

- **CEO & Business Development** : approva la presente politica, assicura la disponibilità delle risorse necessarie al SGSI e promuove la cultura della sicurezza delle informazioni a tutti i livelli dell'organizzazione.
- **Responsabile del sistema di gestione** : coordina la progettazione, l'attuazione e il miglioramento continuo del SGSI, verifica l'aggiornamento e la comunicazione della politica e ne predispone la revisione periodica.
- **Admin & Biz.Dev** : supporta la predisposizione della documentazione gestionale e il coordinamento delle attività amministrative necessarie ai processi di governance del SGSI.

- **Sviluppo Web** : sovrintende all'applicazione delle misure di sicurezza nello sviluppo, nel deployment e nella manutenzione della piattaforma e nelle integrazioni con l'infrastruttura cloud.
- **Sviluppo Backend** : garantisce il rispetto dei requisiti di sicurezza nell'architettura backend, nelle API e nella progettazione e gestione dei database.
- **Data Analysis** : preserva la qualità, l'integrità e la riservatezza dei dati trattati nelle attività di analisi e reportistica.

Impegno e obiettivi del sistema di gestione

Impegno del Top Management

Joinrs S.r.l. considera la sicurezza delle informazioni una componente inscindibile della propria strategia di crescita nel mercato della tecnologia per le risorse umane. Il **CEO & Business Development**, quale massima espressione della direzione aziendale, assume la titolarità degli impegni qui dichiarati e ne garantisce l'attuazione attraverso le attività di governo descritte nella *PRO Processi direzionali* e il riesame periodico del SGSI.

L'organizzazione si impegna a destinare risorse finanziarie, umane e tecnologiche adeguate alla complessità del proprio contesto operativo, affinché il SGSI disponga degli strumenti necessari a raggiungere gli obiettivi fissati. Tale impegno si estende all'integrazione dei requisiti di sicurezza in ogni processo aziendale, dalla progettazione e sviluppo della piattaforma SaaS fino all'erogazione dei servizi di matching basato su intelligenza artificiale e di employer branding.

Joinrs promuove un approccio basato sul rischio, in cui ogni decisione relativa alla protezione degli asset informativi deriva da una valutazione sistematica e documentata delle minacce, delle vulnerabilità e degli impatti, condotta secondo la metodologia definita nella *PRO Procedura di gestione dei rischi*. I risultati delle valutazioni orientano la selezione dei controlli e alimentano il piano di trattamento, approvato dal **CEO & Business Development** e monitorato nel tempo.

L'organizzazione riconosce che la sicurezza delle informazioni è una responsabilità condivisa. Per questo motivo, Joinrs promuove una cultura diffusa della consapevolezza, sostenuta da iniziative di formazione e sensibilizzazione destinate a tutto il personale, proporzionate al ruolo ricoperto. Ciascun dipendente e collaboratore contribuisce attivamente alla protezione degli asset informativi, nel rispetto dei principi sanciti dal *Codice di condotta* e delle politiche e procedure del SGSI.

Joinrs si impegna a soddisfare i requisiti applicabili in materia di sicurezza delle informazioni, siano essi di natura legale, regolamentare o contrattuale, con particolare riferimento alla protezione dei dati personali dei candidati e dei clienti corporate, alle disposizioni sulla resilienza delle infrastrutture digitali e alla normativa sull'intelligenza artificiale. La conformità è perseguita come condizione necessaria per operare in modo responsabile e per preservare la fiducia delle parti interessate.

L'organizzazione adotta il miglioramento continuo come principio guida del SGSI. L'efficacia delle misure di sicurezza è verificata attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli esiti degli audit interni ed esterni, la gestione delle non

conformità e il riesame della direzione condotto secondo la *PRO Gestione riesame della direzione*. Le conclusioni di tali attività alimentano il programma di miglioramento e orientano l'evoluzione degli obiettivi e dei controlli.

Obiettivi di sicurezza delle informazioni

La presente politica stabilisce il quadro entro cui l'organizzazione definisce e riesamina i propri obiettivi di sicurezza delle informazioni. Tali obiettivi, coerenti con gli indirizzi strategici e con il contesto organizzativo, sono i seguenti:

- **Proteggere riservatezza, integrità e disponibilità delle informazioni** gestite dalla piattaforma, dai sistemi di matching basati sull'intelligenza artificiale e dai servizi di employer branding, adottando controlli proporzionati al valore degli asset e al livello di rischio.
- **Assicurare la conformità normativa e contrattuale**, con particolare attenzione alla protezione dei dati personali dei candidati e dei clienti corporate e agli obblighi derivanti dalla disciplina europea in materia di sicurezza delle reti, dei sistemi informativi e dell'intelligenza artificiale.
- **Promuovere una cultura della sicurezza** attraverso attività di sensibilizzazione, formazione e comunicazione continua rivolte a tutto il personale, affinché ciascuno sia consapevole del proprio ruolo nella protezione degli asset informativi.
- **Gestire i rischi in modo sistematico e proattivo**, fondando ogni decisione su valutazioni oggettive e aggiornate e attuando piani di trattamento approvati dalla direzione.
- **Salvaguardare la continuità dei servizi**, garantendo la resilienza dell'infrastruttura cloud e l'efficacia dei meccanismi di prevenzione, rilevamento e risposta agli incidenti di sicurezza.
- **Migliorare costantemente l'efficacia del SGSI**, attraverso il monitoraggio degli indicatori di prestazione, l'analisi degli esiti degli audit, la gestione delle non conformità e il riesame periodico condotto dal **CEO & Business Development**.

Gli obiettivi sono misurati attraverso indicatori specifici, declinati nel programma di miglioramento e riesaminati in occasione del riesame della direzione. La *PRO Procedura delle misurazioni e del monitoraggio* disciplina le modalità di raccolta, analisi e valutazione dei dati a supporto del raggiungimento degli obiettivi.

Comunicazione della politica

Joinrs garantisce che la presente politica sia efficacemente comunicata e resa comprensibile a tutto il personale e alle parti interessate rilevanti. Sul piano interno, la politica è diffusa tramite i canali di comunicazione aziendale, che comprendono la posta elettronica, la messaggistica istantanea, la bacheca digitale interna, sessioni di formazione e riunioni di team, secondo le modalità disciplinate dalla *PRO Procedura gestione comunicazione*; ogni nuovo assunto la riceve durante il processo di inserimento. Sul piano esterno, la politica, classificata come pubblica, è pubblicata sul sito web aziendale, nel footer della pagina, affinché sia accessibile e consultabile da chiunque. Le evidenze di

avvenuta comunicazione, quali registri di presa visione, log delle e-mail e verbali di riunione, sono conservate come informazioni documentate del SGSI.

Archiviazione e aggiornamento

La presente politica è conservata come informazione documentata del SGSI sulla piattaforma documentale aziendale, in formato digitale che ne garantisce l'integrità e la tracciabilità delle revisioni. Il **Responsabile del sistema di gestione** ne cura la revisione almeno una volta all'anno, in concomitanza con il riesame della direzione, oppure ogni qualvolta intervengano cambiamenti significativi nel contesto organizzativo, nel panorama delle minacce, nel quadro normativo o nella strategia aziendale. Ogni aggiornamento è sottoposto all'approvazione formale del **CEO & Business Development** prima della distribuzione. Le versioni superate sono archiviate con indicazione della data di sostituzione, a garanzia della ricostruibilità storica del documento.

Documenti di riferimento

- POL Politica di sicurezza delle informazioni
- PRO Processi direzionali
- PRO Procedura di gestione dei rischi
- PRO Procedura delle misurazioni e del monitoraggio
- PRO Gestione riesame della direzione
- PRO Procedura gestione comunicazione
- Codice di condotta