POLITICA

PL_01

POLITICA SICUREZZA DELLE INFORMAZIONI

POLITICA AZIENDALE DI RIFERIMENTO	**POLITICA SICUREZZA DELLE INFORMAZIONI**
DATA DI APPROVAZIONE DELLA PROCEDURA	15/09/2025
DATA DI ENTRATA IN VIGORE DELLA PROCEDURA	15/09/2025
STATO DELLA PROCEDURA	Revisione 2
DATA DELL'ULTIMA REVISIONE	29/09/2026
DATA DELLA PROSSIMA REVISIONE	Settembre 2027
CLASSIFICAZIONE	Pubblico

JOBCODE STP SRL con sede legale in, Porta Romana 6 a Milano, codice fiscale e partita IVA 10264100966	POLITICA SICUREZZA DELLE INFORMAZIONI
Numero e codice procedurale: PL_01	

Versione	Data	Descrizione	Autore
1	05/03/2025	Prima emissione per implementazione del sistema	RSGSI
2	15/09/2025	Integrazione	RSGSI
3	29/09/2026	Integrazione	CISO

JOBCODE STP SRL con sede legale in, Porta Romana 6 a Milano, codice fiscale e partita IVA 10264100966	POLITICA SICUREZZA DELLE INFORMAZIONI
Numero e codice procedurale: PL_01	

Sommario

1. OGGETTO4
2. AMBITO DI APPLICAZIONE4
3. APPROVAZIONE E SUPERVISIONE DELLA DIREZIONE4
4. RIFERIMENTI NORMATIVI4
5. PRINCIPI E IMPEGNO4
6. PRINCIPI ESG (ENVIRONMENTAL, SOCIAL, GOVERNANCE)6
7. RUOLI, RESPONSABILITÀ E AUTORITÀ7
8. REVISIONE DELLA POLITICA9
9. INFORMAZIONI DI CONTATTO9
10. DISTRIBUZIONE E CONOSCENZA DELLA PRESENTE PROCEDURA9

1. OGGETTO

Il presente documento definisce la politica della sicurezza delle informazioni, requisito della clausola 5.2 della norma ISO/IEC 27001:2022. L'alta direzione emana la strategia definita in questo documento, a cui devono allinearsi tutte le ulteriori politiche, procedure, linee guida, etc.

2. AMBITO DI APPLICAZIONE

Questa politica si applica a tutte le informazioni trattate da Jobcode, in formato elettronico o cartaceo, incluse le informazioni di clienti, fornitori, partner e dipendenti, nonché ai sistemi, applicazioni e processi impiegati per il trattamento di tali dati.

3. APPROVAZIONE E SUPERVISIONE DELLA DIREZIONE

La presente è formalmente documentata ed è stata approvata dall'alta dirigenza dell'azienda. La direzione ne supervisiona l'attuazione e garantisce che tutte le misure di sicurezza siano applicate e verificate in modo coerente. Eventuali modifiche devono essere esaminate e approvate dalla direzione.

4. RIFERIMENTI NORMATIVI

Jobcode assicura la conformità con tutte le leggi e regolamenti applicabili in materia di protezione dei dati personali e sicurezza delle informazioni, tra cui:

1. ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements;
2. ISO/IEC 27001:2022/Amd 1:2024 Amendment 1: Climate action changes
3. Regolamento (UE) 2016/679 "GDPR";
4. Decreto Legislativo 196 del 2003 "Codice in materia di protezione dei dati personali";

5. PRINCIPI E IMPEGNO

Jobcode ha adottato un Sistema di Gestione per la Sicurezza delle Informazioni ai sensi della norma ISO/IEC 27001:2022 al fine di aumentare l'affidabilità nella gestione della sicurezza delle informazioni e nella protezione dei dati.

Jobcode si impegna a garantire la protezione delle informazioni di clienti, dipendenti e partner, assicurando che le informazioni sensibili e personali siano trattate nel rispetto delle normative e degli standard internazionali. La presente politica, in conformità con la norma ISO 27001:2022, definisce gli impegni e gli obiettivi di alto livello in materia di sicurezza delle informazioni:

1. Garantire la riservatezza, integrità e disponibilità delle informazioni.
2. Prevenire accessi non autorizzati, divulgazioni, modifiche o distruzioni delle informazioni.

3. Gestire e ridurre i rischi per la sicurezza delle informazioni attraverso misure di controllo efficaci.
4. Assicurare la conformità con le normative vigenti in materia di protezione dei dati personali (ad esempio GDPR) e sicurezza delle informazioni.
5. Promuovere la consapevolezza della sicurezza delle informazioni tra i dipendenti e i collaboratori.
6. Implementare, certificare e mantenere attivo un sistema di gestione integrato mirato al miglioramento continuo delle prestazioni, integrando la sicurezza delle informazioni nei processi core dell'azienda, come consulenza del lavoro, gestione delle risorse umane e payroll outsourcing.
7. Implementare un approccio basato sul rischio per identificare, valutare e gestire le minacce alla sicurezza delle informazioni, considerando il contesto aziendale e le esigenze delle parti interessate.
8. Stabilire politiche, procedure e controlli di sicurezza delle informazioni adeguati alla natura sensibile dei dati trattati, inclusi dati personali, informazioni finanziarie e dati HR dei clienti.
9. Allineare il sistema di gestione della sicurezza delle informazioni con la visione aziendale e con altre certificazioni e standard aziendali, come la certificazione di parità di genere e l'attestazione ISAE 3402 Type II.
10. Investire nella formazione continua e sensibilizzazione del personale sulla sicurezza delle informazioni.
11. Promuovere una cultura della sicurezza in tutta l'organizzazione attraverso programmi di informazione e formazione.
12. Monitorare i processi tramite opportuni indicatori di performance e stabilire meccanismi per misurare e valutare l'efficacia del sistema di gestione della sicurezza delle informazioni attraverso audit interni e riesami periodici.
13. Migliorare la comunicazione interna ed esterna, favorendo la messa a fattor comune di strumenti e buone prassi tra le articolazioni organizzative.
14. Mantenere sotto controllo il rispetto della normativa vigente, l'aggiornamento e l'adeguamento normativo, assicurando la conformità alle normative italiane e internazionali, incluso il GDPR e altre leggi pertinenti al settore HR e payroll.
15. Ridurre le non conformità alla fonte tramite opportune azioni correttive e preventive.
16. Garantire la sicurezza dei locali e degli strumenti fisici, logistici ed organizzativi atti al trattamento delle informazioni.
17. Proteggere le informazioni trattate implementando controlli fisici, tecnici, organizzativi e sulle persone.
18. Selezionare e monitorare accuratamente i fornitori che erogano servizi/forniscono prodotti ICT.
19. Garantire la business continuity aziendale e il disaster recovery attraverso l'applicazione di procedure di sicurezza e di emergenza stabilite.
20. Definire ruoli, responsabilità e autorità per la sicurezza delle informazioni.
21. Valutare regolarmente i rischi legati alla sicurezza delle informazioni attraverso un processo sistematico di identificazione, analisi e trattamento dei rischi, implementando misure di sicurezza per mitigare i rischi identificati.
22. Far rispettare a dipendenti e collaboratori procedure e controlli di sicurezza delle informazioni e segnalare tempestivamente qualsiasi incidente o violazione.

23. Fornire il supporto necessario per il miglioramento continuo del SGSI e per il raggiungimento degli obiettivi di sicurezza delle informazioni.
24. Stabilire procedure per la gestione degli incidenti di sicurezza delle informazioni, inclusa la rilevazione, la risposta e la notifica di violazioni dei dati.
25. Valutare e migliorare regolarmente il sistema di gestione della sicurezza delle informazioni per garantire che resti adeguato, efficace e conforme agli sviluppi tecnologici e alle nuove minacce.
26. Riesaminare la politica annualmente o quando necessario per garantire che rimanga adeguata agli obiettivi aziendali e alle minacce emergenti.
27. Integrare i requisiti di sicurezza delle informazioni nelle relazioni con i partner del network HLB, i fornitori di tecnologia e altri stakeholder rilevanti.
28. Documentare e mantenere le informazioni necessarie per supportare l'operatività del sistema di gestione della sicurezza delle informazioni e dimostrare la conformità ai requisiti di questo documento.

Jobecode si impegna ad assumere un ruolo attivo nella promozione e guida di tutte le attività aventi influenza sulla sicurezza delle informazioni, attraverso la diffusione a tutti i livelli dei concetti esposti e il continuo monitoraggio e aggiornamento della presente politica e degli obiettivi prefissati.

6. PRINCIPI ESG (ENVIRONMENTAL, SOCIAL, GOVERNANCE)

Jobcode si impegna a integrare i principi di sostenibilità ambientale, responsabilità sociale e buona governance nelle proprie attività, incluse quelle legate alla sicurezza delle informazioni. L'impegno ESG si riflette anche nella sicurezza delle informazioni attraverso un approccio proattivo e a lungo termine che mira a ridurre l'impatto ambientale delle nostre operazioni e a migliorare continuamente la protezione dei dati.

Ambiente
Jobcode riconosce l'importanza della protezione ambientale anche nella gestione della sicurezza delle informazioni, attraverso:

- Digitalizzazione e Riduzione dei Rifiuti: promozione dell'uso di tecnologie digitali sicure per ridurre l'uso di carta e materiali di consumo. I sistemi di gestione delle informazioni sono progettati per minimizzare l'impatto ambientale attraverso l'ottimizzazione delle risorse.
- Efficienza Energetica: I data center e sistemi informatici sono selezionati e gestiti in modo da ridurre il consumo energetico e le emissioni di CO2, scegliendo soluzioni più sostenibili quando possibile.

Responsabilità Sociale
La responsabilità sociale è parte integrante della visione aziendale, come descritto nei valori aziendali:

- Inclusività e Parità di Genere: Jobcode si impegna a garantire la parità di genere e un ambiente di lavoro inclusivo, promuovendo la partecipazione equa di tutti i dipendenti alla sicurezza delle informazioni e assicurando che i ruoli di responsabilità siano aperti a tutti senza discriminazioni.

- Formazione e Consapevolezza: investimento nella formazione continua dei nostri dipendenti e collaboratori per promuovere una cultura della sicurezza delle informazioni, offrendo sessioni di formazione periodiche su tematiche legate alla sicurezza informatica e alla gestione dei dati per favorire la crescita personale e professionale.

Governance
Una gestione trasparente e responsabile è fondamentale per garantire la sicurezza delle informazioni:

- Compliance e Etica: Jobcode garantisce che tutte le decisioni relative alla sicurezza delle informazioni siano prese in conformità con le normative applicabili e con principi etici rigorosi.
- Monitoraggio e Trasparenza: le attività in materia di sicurezza delle informazioni sono regolarmente monitorate e sottoposte a revisione per assicurare il rispetto delle normative e delle migliori pratiche internazionali. L'alta direzione è impegnata a garantire una governance efficace del sistema di gestione della sicurezza delle informazioni, sostenendo pratiche di rendicontazione trasparente.

7. RUOLI, RESPONSABILITÀ E AUTORITÀ

La norma ISO/IEC 27001:2022 richiede che le organizzazioni definiscano chiaramente ruoli, responsabilità e autorità per garantire un'efficace gestione della sicurezza delle informazioni. Jobcode ha strutturato questi ruoli in modo proporzionato, evitando complessità e garantendo una chiara suddivisione dei compiti, individuando tre figure fondamentali: CISO (Chief Information Security Officer), RSGSI (Responsabile Sistema di Gestione Sicurezza delle Informazioni) e Supporto IT (Team Help Desk).

CISO (Chief Information Security Officer)
Responsabile strategico della sicurezza informatica e della gestione dei rischi.
Responsabilità:

- Definire la strategia di sicurezza delle informazioni in linea con gli obiettivi aziendali.
- Identificare, valutare e mitigare i rischi per la sicurezza informatica.
- Supervisionare la gestione delle minacce e degli incidenti di sicurezza.
- Garantire l'adeguatezza delle misure di sicurezza tecniche e organizzative.
- Assicurare la conformità normativa e la gestione delle relazioni con le parti interessate (es. clienti, fornitori, autorità).

Autorità:

- Approva misure di sicurezza e controlli tecnici.
- Approva strategia di sicurezza e obiettivi.
- Autorizza gli investimenti in sicurezza.

Responsabile SGSI
Responsabile della conformità e della gestione del SGSI.

Responsabilità:

- Definire, implementare e mantenere il SGSI.
- Monitorare il miglioramento continuo del sistema e la gestione dei rischi.
- Redigere e aggiornare le politiche di sicurezza delle informazioni.
- Pianificare e supervisionare gli audit interni ISO 27001.
- Formare e sensibilizzare il personale sulla sicurezza delle informazioni.
- Gestire la documentazione del SGSI.

Autorità:

- Autorizza gli aggiornamenti alle politiche di sicurezza.
- Ha accesso ai risultati degli audit e può segnalare non conformità.
- Può richiedere interventi correttivi ai responsabili di processo.

Responsabili della struttura IT
L'Infrastruttura IT è gestita internamente avvalendosi di aziende esterne un Team di Helpdesk/Supporto IT. Per garantire la conformità ai requisiti della norma ISO 27001:2022, Ventunocento e il Team di Helpdesk/Supporto IT operano in stretta collaborazione, mantenendo una comunicazione continua e strutturata attraverso un sistema di ticketing dedicato. Questo approccio assicura la tracciabilità delle richieste, la gestione efficace degli incidenti e il rispetto delle politiche di sicurezza delle informazioni.
Ventunocento gestisce e assicura il corretto funzionamento dell'infrastruttura IT aziendale, implementando le misure di sicurezza tecniche necessarie per proteggere i sistemi e i dati.

Di seguito vengono illustrate le responsabilità del Team di Helpdesk/Supporto IT.

- Amministrare l'infrastruttura IT (server, reti, sistemi operativi, applicazioni, ecc.).
- Implementare e monitorare le misure di sicurezza informatica (firewall, antivirus, backup, crittografia, ecc.).
- Garantire la conformità tecnica ai requisiti di sicurezza stabiliti dal CISO e dal Responsabile SGSI.
- Gestire gli accessi ai sistemi e garantire il principio del least privilege.
- Monitorare e rispondere agli incidenti di sicurezza informatica.

Autorità:

- Approva ed esegue modifiche di routine alle configurazioni su sistemi e reti.
- Approva, revoca o modifica gli accessi.

Team Help Desk/Supporto IT

- Monitorare e rispondere agli incidenti di sicurezza informatica.
- Mantenere e aggiornare i sistemi in conformità con le policy aziendali.
- Supportare la formazione tecnica sulla sicurezza per i dipendenti.
- Segnala problemi di sicurezza alla direzione e proporre investimenti in infrastruttura tecnologica.

8. REVISIONE DELLA POLITICA

Questo documento viene rivisto annualmente o secondo necessità a causa di cambiamenti nelle operazioni o rischi per la sicurezza. Tutti gli aggiornamenti saranno comunicati ai dipendenti e, se necessario, verrà fornita una nuova formazione per garantire il rispetto continuo delle più recenti misure di sicurezza.

9. INFORMAZIONI DI CONTATTO

Per domande relative a questo documento, si prega di contattare il responsabile della sicurezza delle informazioni tiziana.savoia@jobcodehr.com.

10. DISTRIBUZIONE E CONOSCENZA DEL PRESENTE DOCUMENTO

Il presente documento è condiviso con tutto il personale tramite Intranet aziendale e con le parti interessate esterne tramite sito aziendale.

Approvato dalla Direzione _____

JOBCODE STP SRL
Corso di Porta Romana, 6 20122 Milano
C. F. e P. IVA 10264100966