

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 1 di 6

1. PREMESSA

GIOBBY srl è una startup costituita a Ottobre 2025. Già avviata grazie al gestionale GIOBBY progettato per la fatturazione elettronica. Il suo core business è la commercializzazione di software in SaaS con l'utilizzo di sistemi di intelligenza artificiale per la gestione aziendale.

2. SCOPO

Giobby srl S.r.l., ha deciso di sviluppare un Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) in conformità allo standard internazionale ISO/IEC 27001:2022 al fine di tutelare il suo patrimonio di conoscenza, le sue soluzioni informatiche e più in generale il suo sistema informativo e documentale dalle molteplici minacce interne ed esterne, intenzionali o accidentali attraverso un processo continuo di gestione dei rischi.

Il presente documento definisce la politica aziendale per la sicurezza delle informazioni.

Il rispetto dei contenuti della presente politica è da considerarsi obbligatorio per tutto il personale e deve far parte delle dichiarazioni di impegno con qualsiasi soggetto esterno che, a qualsiasi titolo, possa essere coinvolto nel trattamento delle informazioni che rientrano nel contesto di applicazione del SGSI.

3. CAMPO DI APPLICAZIONE

Il campo di applicazione del SGSI nello specifico dominio aziendale di Giobby srl S.r.l., relativamente al suo contesto operativo si applica a tutte le funzioni aziendali ma si declina in misura specifica nel seguente perimetro:

Servizi di erogazione ed assistenza di servizi Cloud (SaaS) con sistemi di intelligenza artificiale in accordo alla Dichiarazione di Applicabilità rev. 0 del 23/01/2026

4. RIFERIMENTI NORMATIVI & CONTRATTUALI

NORME E LEGGI	DESCRIZIONE
ISO IEC 27000	Information security, cybersecurity and privacy protection - Information security management systems - Requirements

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 2 di 6

ISO IEC 27002	Information security, cybersecurity and privacy protection — Information security controls
D.Lgs. 196/2003	
Regolamento UE 2016/679	GDPR

5. OBIETTIVI

L'obiettivo principale di dotarsi di un SGSI è garantire un adeguato livello di sicurezza delle informazioni (comprendendo i dati personali) nell'ambito di tutte le fasi del trattamento delle stesse (acquisizione, elaborazione, progettazione, conservazione, trasmissione, eventuale distruzione, ecc.) in linea con l'analisi dei rischi e con le "best practices" attuate dall'organizzazione. Un SGSI definisce un insieme di misure organizzative, logistiche, informatiche e comportamentali atte a garantire:

- ✓ la confidenzialità o riservatezza delle informazioni: ovvero le informazioni devono essere accessibili solo da chi è autorizzato e ne ha i privilegi;
- ✓ l'integrità delle informazioni: ovvero proteggere la qualità e la completezza delle informazioni e l'affidabilità dei metodi per la loro elaborazione;
- ✓ la disponibilità delle informazioni: ovvero garantire l'accesso alle informazioni e alle risorse collegate da parte degli utenti autorizzati nel momento in cui lo richiedono.

Attraverso la comunicazione del presente documento, la Direzione intende perseguire dieci obiettivi generali:

- ✓ standardizzare una metodologia di analisi del rischio sulla sicurezza delle informazioni;
- ✓ perseguire il miglioramento continuo attraverso l'implementazione di un SGSI certificato ISO27001;
- ✓ proteggere il proprio patrimonio informativo e le sue informazioni aziendali;
- ✓ aumentare il senso di consapevolezza e responsabilità nel personale e nei collaboratori relativamente alle tematiche connesse la sicurezza delle informazioni;
- ✓ preservare la brand reputation;
- ✓ soddisfare le aspettative della clientela fornendo garanzie e rassicurazioni sul livello di affidabilità e sicurezza delle loro informazioni;

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 3 di 6

- ✓ tutelarsi da eventuali rischi di natura legale (comprendendo eventuali penali contrattuali) dovuti a violazioni sulla sicurezza delle informazioni;
- ✓ conformarsi ai requisiti internazionali sulla sicurezza delle informazioni richiesti esplicitamente dai clienti favorendo al contempo lo sviluppo di nuove opportunità di business;
- ✓ garantire un'integrazione efficace tra i requisiti volontari della ISO 27001 e i requisiti cogenti del Regolamento UE 2016/679 e più in generale della normativa sul trattamento dei dati personali;
- ✓ rispondere pienamente ai requisiti cogenti e normativi volontari sul tema della sicurezza delle informazioni.

Contestualizzando lo scopo della Direzione nel dominio operativo di Giobby S.r.l., rispetto all'oggetto di tale documento, l'obiettivo che naturalmente ne consegue è quello di rendere evidente l'impegno profuso della società in ambito sicurezza e affidabilità dei propri servizi e concretizzarlo formalmente nella certificazione ISO27001.

Il raggiungimento della certificazione ISO 27001 certificherà al mercato l'impegno di Giobby S.r.l. in ambito sicurezza informatica, renderà possibile la finalizzazione di accordi che prevedono tali livelli di certificazione come obbligatori e costituirà una garanzia ulteriore per i clienti che già utilizzano i sistemi ed i servizi di Giobby S.r.l.

Gli obiettivi specifici e tecnici che Giobby S.r.l. si impegna a raggiungere, il contesto nel quale opera e tutte le azioni che saranno messe in campo sono oggetto del SGSI, dei relativi documenti specifici.

6. IMPEGNO DELLA DIREZIONE

Giobby S.r.l. ritiene che la sicurezza delle informazioni rappresenti un fattore critico di successo sia per quanto riguarda i processi di progettazione e sviluppo di soluzioni tecnologiche che per quanto riguarda l'erogazione dei servizi.

La Direzione è impegnata nel processo di responsabilizzazione delle risorse e verificherà periodicamente e regolarmente (o in concomitanza di cambiamenti significativi normativi e organizzativi) l'efficacia e l'efficienza del Sistema di Gestione della Sicurezza delle Informazioni, riesaminando la politica ed aggiornando l'analisi dei rischi sulle informazioni al fine di individuare e adottare le opportune azioni migliorative. L'impegno della direzione si concretizza tramite una struttura organizzativa i cui compiti sono:

- ✓ garantire che siano identificati tutti gli obiettivi relativi alla sicurezza delle informazioni in aderenza con le politiche e le strategie della società;

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 4 di 6

- ✓ dotarsi di un approccio sistematico per l'analisi del rischio sulle informazioni;
- ✓ ridurre al minimo la probabilità e gli impatti derivanti da incidenti sulla sicurezza delle informazioni;
- ✓ incrementare, in un'ottica di "accountability", i livelli di sicurezza nel trattamento dei dati personali;
- ✓ favorire un'efficace integrazione tra i requisiti di sicurezza delle informazioni e i requisiti obbligatori della normativa italiana (D. Lgs. 196/2003 armonizzato con il D. Lgs. 101/2018) ed europea (Regolamento UE 2016/679) sul trattamento dei dati personali;
- ✓ fornire risorse sufficienti per la pianificazione, implementazione, controllo e miglioramento continuo del SGSI;
- ✓ definire i ruoli e le responsabilità aziendali per la progettazione, miglioramento e mantenimento del SGSI;
- ✓ monitorare le prestazioni del SGSI e assicurare un sistema di risposta veloce ed efficace nella gestione degli incidenti sulla sicurezza delle informazioni;
- ✓ monitorare i cambiamenti dell'esposizione alle minacce, rivedendo i criteri per l'accettazione del rischio e i livelli di rischio accettabili;
- ✓ garantire programmi di informazione, sensibilizzazione e formazione del personale creando una cultura aziendale sulla sicurezza delle informazioni;
- ✓ definire procedure, istruzioni operative e linee guida comportamentali per assicurare la riservatezza, integrità e disponibilità delle informazioni;
- ✓ eseguire audit periodici per verificare il rispetto dei requisiti del SGSI.

La direzione si impegna a divulgare la politica sulla sicurezza delle informazioni e a fornire adeguate risorse al fine di garantire il raggiungimento degli obiettivi del SGSI nell'ottica del miglioramento continuo.

7. POLITICA

Il patrimonio informativo della società è costituito dall'insieme di informazioni (comprendendo i dati personali) trattati attraverso le varie modalità manuali e telematiche.

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 5 di 6

Il contesto nel quale operiamo ci impone, al di là degli obblighi contrattuali, una spiccata attenzione e sensibilità alla sicurezza delle informazioni per tutelare la nostra brand reputation, garantire l'aderenza alla normativa privacy europea, prevenire cause legali e danni patrimoniali ed andare incontro alle aspettative dei nostri clienti sempre più esigenti in tal senso.

Giobby S.r.l. per soddisfare le esigenze di sicurezza sulle informazioni esegue periodicamente l'analisi dei rischi al fine di individuare eventuali ambiti di miglioramento che possono interessare i processi, gli strumenti, le procedure organizzative, le risorse, i rapporti con i partner e la tipologia di informazioni trattate e comunicate internamente ed esternamente dall'organizzazione.

I principi base cui si basa la nostra politica sulla sicurezza delle informazioni comprendono i seguenti principi cardini:

- ✓ la conformità ai requisiti legislativi e le normative legate alla sicurezza delle informazioni;
- ✓ la continua comunicazione, sensibilizzazione e formazione del personale al fine di favorire la consapevolezza e la conoscenza interna sull'importante e strategica tematica della sicurezza delle informazioni;
- ✓ un puntuale censimento e identificazione degli asset aziendali (le informazioni strategiche trattate e gli strumenti utilizzati per i trattamenti);
- ✓ l'adozione di un sistema di classificazione delle informazioni;
- ✓ l'adozione di un sistema di identificazione, analisi e trattamento dei rischi sulla sicurezza delle informazioni;
- ✓ un continuo bilanciamento di interessi tra l'esigenza di condividere la conoscenza all'interno della società e l'esigenza di garantire la sicurezza delle informazioni; in tal senso la sicurezza delle informazioni non deve pregiudicare l'efficienza e lo scambio di conoscenza come valore aggiunto nella gestione dei progetti;
- ✓ la definizione di chiare e vincolanti clausole contrattuali e accordi di riservatezza sulla sicurezza delle informazioni con i collaboratori, fornitori e i clienti della società;
- ✓ il rispetto di procedure e sistemi di controllo atti a prevenire l'accesso alle informazioni da parte di terzi non autorizzati;
- ✓ l'adozione di un sistema reattivo di gestione degli incidenti sulla sicurezza delle informazioni perfettamente integrato con il processo del Data Breach;
- ✓ l'attuazione di misure idonee di sicurezza informatiche per garantire: la protezione da codici malevoli (antivirus), la disponibilità delle informazioni (backup & recovery) e la riservatezza delle informazioni (firewall, intrusion prevention system, logging, crittografia, ecc.);
- ✓ la predisposizione di piani di disaster & recovery e business continuity per favorire la continuità operativa in caso di eventi bloccanti imprevisti, garantendo il ripristino dei servizi critici in tempi e con modalità che limitino il più possibile le conseguenze negative;
- ✓ la predisposizione di procedure aziendali per lo sviluppo sicuro del software;

	Sistema di Gestione della Sicurezza delle Informazioni ISO/IEC 27001	N. Mod.:	Allegato 3 MI
		Rev.:	0 del 19-02-2026
		CLASS E	PUBBLICO
POLITICA PER LA SICUREZZA DELLE INFORMAZIONI			Pag. 6 di 6

- ✓ la predisposizione di strumenti di monitoraggio, controllo e audit interni per verificare il rispetto degli obiettivi prefissati sulla sicurezza delle informazioni e delle disposizioni della normativa ISO 27001;
- ✓ la promozione di programmi di miglioramento continui del sistema di gestione per la sicurezza delle informazioni.

8. RIESAME DELLA DIREZIONE

La Direzione verificherà ad intervalli pianificati il SGSI per assicurarne la continua idoneità, adeguatezza ed efficacia in concomitanza con la politica e gli obiettivi stabiliti e i cambiamenti significativi interni (organizzativi, ecc.) ed esterni (nuove minacce, cambiamenti legislativi, ecc.) al fine di favorire un processo continuo di innovazione e miglioramento in totale aderenza con i principi cardini del Regolamento UE 2016/679.

I risultati della valutazione del rischio e il piano del trattamento del rischio insieme ai risultati delle attività di controllo (monitoraggio, audit, ecc.) così come le informazioni di ritorno delle parti interessate, completeranno gli elementi di ingresso del riesame strumentali l'adozione di opportunità di miglioramento o necessità di modifiche al SGSI.

Gli *output* del riesame saranno condivisi con i responsabili di funzione definendo obiettivi specifici e fornendo al contempo l'opportunità di valutare come il sistema di gestione stia funzionando.

Data: 19/02/2026

La Direzione

