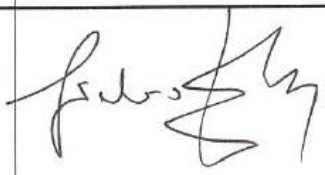
	Nome	Data	Firma
Emessa da	Giulio Fadda (RSG)	19/11/2024	
Verificata da	Giulia Martinelli (AUD)	19/11/2024	
Approvata da	Pablo Liuzzi (CEO)	19/11/2024	

Sommario

PREMESSA

Tecnolife It Consulting S.r.l. nasce nel 2013 come un'azienda di consulenza strutturata in Software Factory distinte per ambito tecnologico che si occupano della consulenza, progettazione e realizzazione di soluzioni IT in ambito Enterprise ed E-commerce.

L'ambito IT si declina in due Software Factory che sviluppano soluzioni su tecnologie Java e app mobile ibride e native. In ambito e-commerce, in qualità di Adobe Solutions Partner, la Società è specializzata nella progettazione di piattaforme e-commerce personalizzate e multicanale per aziende B2C (buisness to consumer) e B2B (buisness to buisness).

1. SCOPO

Tecnolife It Consulting S.r.l., già certificata per lo standard internazionale UNI EN ISO 9001:2015, 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, i suoi progetti, 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.

2. CAMPO DI APPLICAZIONE

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

- *Progettazione, sviluppo e rilascio di soluzioni informatiche web based ed e-commerce con erogazione dei relativi servizi di assistenza tecnica e supporto formativo in accordo alla Dichiarazione di Applicabilità rev. 1 del 3/5/2023*

3. RIFERIMENTI NORMATIVI & CONTRATTUALI

- ISO IEC 27000
  Information technology - Security techniques - Information security management systems - Overview and vocabulary

- ISO IEC 27001
  Information security, cybersecurity and privacy protection - Information security management systems - Requirements

- ISO IEC 27002
  Information security, cybersecurity and privacy protection — Information security controls

- D. Lgs. 196/2003

- Regolamento UE 2016/679

4. 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:

1. standardizzare una metodologia di analisi del rischio sulla sicurezza delle informazioni;

2. perseguire il miglioramento continuo attraverso l'implementazione di un SGSI certificato ISO27001;
3. proteggere il proprio patrimonio informativo e le sue informazioni aziendali;
4. aumentare il senso di consapevolezza e responsabilità nel personale e nei collaboratori relativamente alle tematiche connesse la sicurezza delle informazioni;
5. preservare la brand reputation;
6. soddisfare le aspettative della clientela fornendo garanzie e rassicurazioni sul livello di affidabilità e sicurezza delle loro informazioni;
7. tutelarsi da eventuali rischi di natura legale (comprendendo eventuali penali contrattuali) dovuti a violazioni sulla sicurezza delle informazioni;
8. conformarsi ai requisiti internazionali sulla sicurezza delle informazioni richiesti esplicitamente dai clienti favorendo al contempo lo sviluppo di nuove opportunità di business;
9. 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;
10. rispondere pienamente ai requisiti cogenti e normativi volontari sul tema della sicurezza delle informazioni.

Contestualizzando lo scopo della Direzione nel dominio operativo di Tecnolife It Consulting S.r.l., rispetto all'oggetto di tale documento, l'obbiettivo 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 Tecnolife It Consulting 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 Tecnolife It Consulting S.r.l.

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

5. IMPEGNO DELLA DIREZIONE

Tecnolife It Consulting 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;
- 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 efficacie 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.

6. ORGANIGRAMMA DEL SGSI

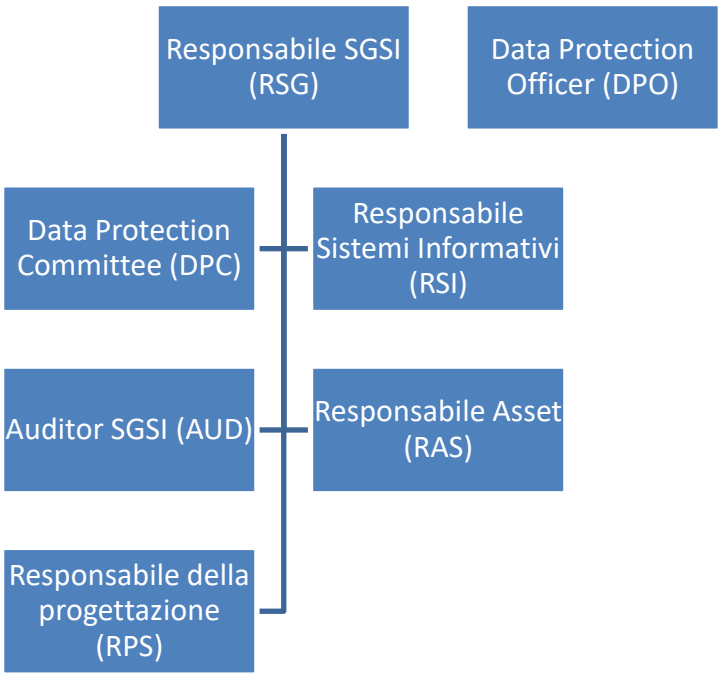


FIGURA	RESPONSABILITA'
Responsabile SGSI (RSG)	È la figura direzionale che coordina le attività di progettazione e implementazione del Sistema di Gestione della Sicurezza delle Informazioni (SGSI) Assicura che il SGSI sia conforme alla normativa ISO27001 e riferisce al Consiglio di Amministrazione sulle prestazioni del sistema. Identifica il Responsabile del SGSI e si adopera per promuovere la competenza e la consapevolezza interna
Responsabile IT (RSI)	È il Responsabile dei sistemi informativi e supervisiona tutte le attività legate alla sicurezza delle informazioni in ambito telematico definendo le procedure di propria pertinenza (Disaster & Recovery, Backup, ecc.) Supporta attivamente l'auditor interno nell'analisi dei rischi e nella definizione di programmi di miglioramento a favore dell'integrità, disponibilità e riservatezza delle informazioni

	È responsabile delle attività di assistenza tecnica, coordina gli amministratori di sistema e si adopera per mettere in atto tutte le misure di sicurezza informatiche previste dal SGSI
Auditor sulla sicurezza delle informazioni (AUD)	È la figura professionale responsabile delle attività di progettazione, disegno, implementazione, training, audit e certificazione del SGSI. Rappresenta l'interfaccia ufficiale nei confronti dell'ente di certificazione terzo Supporta tutte le funzioni nell'implementazione e monitoraggio del sistema secondo i requisiti della ISO 27001
Data Protection Committee (DPC)	Collabora attivamente con l'auditor interno sulla sicurezza delle informazioni nelle attività trasversali la privacy e il data protection in genere. Ha un ruolo di primo piano nella definizione delle policy di sicurezza dei dati e delle informazioni per i collaboratori della società. Funge da CIRT (Computer Incident Response Team) in caso di gestione degli incidenti sulla sicurezza delle informazioni
Responsabile Asset (RAS)	È responsabile di tutti gli asset della società. Esegue il censimento degli asset e mantiene aggiornato l'inventario degli asset della società
Responsabile Progettazione SW	È il responsabile del reparto di sviluppo sw. Integra l'approccio security & privacy by design nei Progetti. Verifica che lo sviluppo del sw avvenga secondo i principi di sviluppo sicuro
DPO	È il responsabile della protezione dei dati personali nominato ai sensi dell'art. 37 del Reg. UE 2016/679. È la figura istituzionale ufficiale interna per la protezione dei dati personali.

Ente di Certificazione	Rappresenta l'ente terzo accreditato da Accredia per la valutazione e il rilascio del certificato ISO27001. Esegue le attività di audit di terza parte strumentali l'ottenimento del certificato e il mantenimento dello stesso nell'ambito di ogni triennio.

ORGANIGRAMMA NOMINALE:

FUNZIONE	NOMINATIVO
CEO	Pablo Liuzzi
Responsabile Sicurezza delle Informazioni	Giulio Fadda
Data Protection Officer	Laura Mariani
Auditor Sicurezza delle Informazioni	Giulia Martinelli
Responsabile Progettazione Sw	Davide Marino
Data Protection Committee	Giulio Fadda, Giulia Martinelli, Davide Marino
Responsabile degli Asset	Luna Manili

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.

Il contesto nel quale operiamo ci impone, aldilà 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.

Tecnolife It Consulting 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:

a) la conformità ai requisiti legislativi e le normative legate la sicurezza delle informazioni;
b) 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;
c) l'attivazione di sistemi di threat intelligence per sviluppare la cyber resilienza all'interno dell'organizzazione;
d) l'adozione di un disciplinare informatico interno contenente le linee guida da rispettare in merito al corretto trattamento delle informazioni con modalità telematiche;
e) la partecipazione attiva di tutti i collaboratori della società che in modo propositivo e proattivo possono proporre azioni migliorative e segnalare criticità attraverso lo strumento dedicato di "*Issue Security Log*";
f) un puntuale censimento e identificazione degli asset aziendali (le informazioni strategiche trattate e gli strumenti utilizzati per i trattamenti);
g) l'adozione di un sistema di classificazione delle informazioni;
h) l'adozione di un sistema di identificazione, analisi e trattamento dei rischi sulla sicurezza delle informazioni;
i) l'adozione di un sistema data leakage prevention, data masking e data retention;
j) 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;
k) 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;
l) il rispetto di procedure e sistemi di controllo atti a prevenire l'accesso alle informazioni da parte di terzi non autorizzati;
m) l'adozione di un sistema reattivo di gestione degli incidenti sulla sicurezza delle informazioni perfettamente integrato con il processo del Data Breach;
n) 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.);
o) 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;
p) la predisposizione di procedure aziendali per lo sviluppo sicuro del software;

q) 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;
r) 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: 16/09/2024

La Direzione: _____