SURETY SHIELD SRL
Rev. 00 del 05.05.2025
Politica SGSI ISO/IEC 27001:2022

POLITICA SICUREZZA DELLE INFORMAZIONI ISO 27001:2022

Storia delle modifiche e livello confidenzialità						
Rev	**Data**	**Versione**	**Emesso da**	**Approvato da**	**Descrizione modifica**	**Livello Confidenzialità**
00	05.05.2025	Prima emissione	DG	DPO	-	PUBBLICA

SURETY SHIELD S.r.l. opera sul mercato italiano dal mese di Dicembre 2024. Nata dalla cessione di ramo d'azienda di Cetif Advisory S.r.l., la società è proprietaria e gestore della Piattaforma Fideiussioni Digitali.
Tecnologicamente all'avanguardia, gestisce un mercato con esigenze e caratteristiche specifiche, pensata per rispondere alle esigenze di istituzioni finanziarie e compagnie assicurative offrendo efficienza, trasparenza e conformità normativa.
Il progetto Fideiussioni Digitali risponde al bisogno di:
1. Digitalizzare la gestione del ciclo di vita delle garanzie
2. Proteggere da rischi di manomissioni delle garanzie
3. Contrastare le frodi in tema di gestione delle garanzie
4. Semplificare gli scambi e la possibilità di consultare documenti fideiussori

Fideiussioni Digitali, costruita per fornire un servizio di sistema per garanti, garantiti e contraenti con l'obiettivo di offrire vantaggi e servizi di interesse per gli operatori del settore, è una soluzione innovativa e specializzata nella gestione digitale del processo di emissione e gestione del ciclo di vita delle garanzie fideiussorie.
Sviluppata attraverso l'approccio eco-sistemico di Cetif Advisory, Fideiussioni Digitali vede la collaborazione tra Istituzioni Finanziarie, Compagnie Assicurative, Aziende, Enti ed Autorità.
La sicurezza delle informazioni di tutti i dati trattati da Surety Shield Srl e la protezione della privacy dei clienti è per noi essenziale, per questo abbiamo intrapreso il percorso di certificazione del sistema di gestione della sicurezza delle informazioni secondo la norma ISO IEC 27001:2022.

Lo stesso impegno che poniamo ogni giorno per la tutela della riservatezza, integrità e disponibilità dei dati lo pretendiamo da tutti i nostri dipendenti, collaboratori, fornitori, partner e più in generale da tutti gli stakeholders.
Ci impegniamo ad assicurare la piena e sistematica conformità di tutti i servizi erogati ai nostri clienti ai requisiti cogenti, regolamentari, contrattuali, tecnici applicabili in materia di sicurezza delle informazioni, incluse le informazioni classificate come dati personali e particolari in conformità al GDPR.
Abbiamo adottato una specifica politica per protezione dei dati personali in conformità al GDPR, che costituisce parte integrante della presente politica ed è comunicata a tutti gli stakeholders.
Ci impegniamo a perseguire obiettivi di sicurezza delle informazioni e di protezione dei
dati personali in conformità ai requisiti cogenti applicabili.
La direzione di SURETY SHIELD SRL si impegna a mantenere attiva e a supportare in linea con gli obiettivi aziendali, a tutti i livelli della propria organizzazione, la presente Politica per la Sicurezza delle Informazioni e a divulgarla a tutti gli stakeholder.

Il sistema di gestione della sicurezza delle informazioni preserva la riservatezza, l'integrità e la disponibilità delle informazioni applicando un processo di gestione del rischio e dando fiducia alle parti interessate che i rischi sono adeguatamente gestiti.

SURETY SHIELD SRL identifica tutte le esigenze di sicurezza tramite l'analisi dei rischi che consente di acquisire consapevolezza sul livello di esposizione a minacce del proprio sistema informativo. La valutazione del rischio permette di valutare le potenziali conseguenze e i danni che possono derivare dalla mancata applicazione di misure di sicurezza al sistema informativo e quale sia la realistica probabilità di attuazione delle minacce identificate.
Adottiamo le linee guida in materia di gestione della conformità normativa rappresentata dello standard ISO 37301 «Compliance management systems — Guidelines» e applichiamo lo standard ISO 31000 "Gestione del rischio – principi e linee guida" per la gestione dei rischi inerenti la protezione dei dati personali e le linee guida dello standard ISO/IEC 29134 «Information technology — Security techniques — Guidelines for privacy impact assessment».
I risultati di questa valutazione determinano le azioni necessarie per gestire i rischi individuati e le misure di sicurezza più idonee.

Abbiamo provveduto a nominare un Referente interno per la privacy, un responsabile per la sicurezza IT, un Responsabile della Protezione dei Dati (DPO) ai sensi degli artt. da 37 a 39 del GDPR.
Provvediamo a nominare con apposito atto i nostri responsabili esterni del trattamento ai sensi dell'art. 28 del GDPR, nonché provvediamo a nominare gli incaricati al trattamento ai sensi dell'art. 29 GDPR fornendo istruzioni, formazione, procedure operative e politiche.
Abbiamo nominato l'amministratore di sistema ai sensi del Provvedimento a carattere generale del 27 novembre 2008 (G.U. n. 300 del 24 dicembre 2008).

Predisponiamo un piano di continuità che ci permetta di affrontare efficacemente un evento imprevisto, garantendo il ripristino dei servizi critici in tempi e con modalità che limitano le conseguenze negative sulla missione aziendale.
Abbiamo Procedure operative e linee guida per la gestione di incidenti di sicurezza e per la gestione delle richieste degli interessati.
Gli aspetti di sicurezza sono inclusi in tutte le fasi di progettazione, sviluppo, esercizio, manutenzione, assistenza e dismissione dei sistemi e dei servizi informatici.
Sono garantiti il rispetto delle disposizioni di legge, di statuti, regolamenti o obblighi contrattuali e di ogni requisito inerente la sicurezza delle informazioni, con l'obiettivo di ridurre al minimo il rischio di sanzioni legali o amministrative, di perdite rilevanti o danni alla reputazione.
L'osservanza e l'attuazione della presente Politica e in generale delle procedure aziendali volte a garantire la sicurezza delle informazioni sono responsabilità di tutto il personale dipendente, i collaboratori, partner e fornitori che, a qualsiasi titolo, collaborano con l'azienda e sono coinvolti nel trattamento di dati ed informazioni che rientrano nel campo di applicazione del Sistema di Gestione.
La Direzione verificherà periodicamente e regolarmente o in concomitanza di cambiamenti significativi l'efficacia e l'efficienza del Sistema di Gestione, in modo da assicurare un supporto adeguato all'introduzione di tutte le azioni di miglioramento necessarie e in modo da favorire l'attivazione di un processo di miglioramento continuo, con cui viene mantenuto il controllo e l'adeguamento della politica in risposta ai cambiamenti dell'ambiente aziendale, del business, delle condizioni legali.
I nostri obiettivi per la sicurezza delle informazioni si declinano in obiettivi di preservazione di riservatezza, integrità e disponibilità delle informazioni; in aggiunta, possono essere coinvolte anche altre proprietà quali autenticità, responsabilità, non misconoscimento e affidabilità.
Obiettivi di riservatezza: le informazioni non sono rese disponibili o divulgate a individui, entità, o processi non autorizzati.
Obiettivi di Integrità: salvaguardare l'accuratezza e la completezza dei beni.
Obiettivi di disponibilità: informazioni accessibili e utilizzabili su richiesta di un'entità autorizzata. Gli obiettivi di disponibilità includono obiettivi di resilienza.
Abbiamo effettuato la valutazione dei rischi e delle opportunità per la sicurezza delle informazioni e abbiamo definito un processo di trattamento del rischio per la sicurezza delle informazioni e definito obiettivi per funzioni e livelli pertinenti.
Abbiamo adottato una specifica politica per la continuità operativa. Tale politica costituisce parte integrante della presente politica.
Ci impegniamo ad adeguare e a migliorare continuamente il nostro Sistema di Gestione per la Sicurezza delle Informazioni e a sensibilizzare e formare i nostri dipendenti e partner in merito alla sua corretta applicazione.
Le violazioni della presente politica e del sistema di gestione per la sicurezza delle informazioni da questa richiamato implicano l'applicazione di provvedimenti disciplinari per i dipendenti e di risoluzione dei rapporti contrattuali in essere per collaboratori e professionisti.
Per ogni segnalazione di vulnerabilità, di minaccia, di miglioramento, di non conformità, di incidente, di violazione, di data breach potete contattarci al seguente indirizzo email: asorrentino@fideiussionidigitali.it

oppure potete rivolgervi al Responsabile della protezione dei dati che è contattabile al seguente indirizzo di posta elettronica certificata: privacy@goaps.it.
Ci impegniamo ad assicurare la riservatezza delle segnalazioni e a proibire qualsiasi forma di ritorsione nei confronti dei soggetti segnalanti.
La presente politica è comunicata a tutti i nostri stakeholders ed è disponibile sul nostro sito internet.

L'Alta Direzione

_____

Antonio Sorrentino
Amministratore Delegato
Surety Shield S.r.l.