# Politica generale della Sicurezza delle Informazioni e della Qualità

Bookmark S.r.l. - società a socio unico (di seguito **Bookmark**) è una software house dedita alla progettazione e sviluppo di software gestionali che nasce nel 2001. È composta da un team di esperti di organizzazione, analisti informatici, sviluppatori e specialisti delle nuove tecnologie, che cooperano per il raggiungimento dei risultati attesi dai clienti, nonché dei macro-obiettivi fissati con l'Alta Direzione. Nel 2021 Bookmark entra a far parte del Gruppo Zucchetti.

Bookmark si occupa di produzione di software gestionali e servizi Saas, nonché assistenza, supporto e manutenzione dei servizi erogati. L'azienda offre perciò sistemi e servizi informatici ai propri clienti appartenenti a tutti i settori di mercato.

La Direzione di Bookmark ritiene indispensabile:

- erogare prodotti e servizi di alta qualità, soddisfacendo le esigenze dei clienti e migliorando costantemente le proprie prestazioni;
- garantire la massima sicurezza dei dati trattati e delle informazioni coinvolte nei processi dell'Organizzazione.

A tale scopo Bookmark ha strutturato un Sistema di Gestione Integrato della Qualità e della Sicurezza della Informazioni, certificato ai sensi delle norme ISO 9001 e ISO 27001 integrato dai controlli previsti dalle Linee Guida ISO 27017 e ISO 27018.

In particolare l'organizzazione provvede all'adeguamento continuo dei sistemi, dei processi e delle misure di controllo in conformità ai requisiti delle Linee Guida ISO/IEC 27018:2025, recependo tempestivamente gli aggiornamenti applicabili e garantendone la corretta implementazione e il monitoraggio nel tempo.

Inoltre, Bookmark è stata identificata dall'Agenzia per la Cybersicurezza Nazionale come soggetto essenziale ai sensi della Direttiva NIS2, operando nel settore delle *Infrastrutture digitali* in qualità di fornitore di servizi di cloud computing e nel settore della *Gestione dei servizi TIC* come fornitore di servizi gestiti. Tale qualificazione comporta l'obbligo di adottare adeguate misure tecniche e organizzative per la gestione dei rischi di cybersicurezza, nonché di notificare tempestivamente all'autorità competente eventuali incidenti significativi.

Il documento di Politica si propone di essere uno strumento informativo attendibile, trasparente ed efficace, disponibile per la consultazione online, per rendere consapevoli tutte le parti interessate, interne ed esterne a Bookmark, circa il proprio sistema di gestione integrato.

## Campo di applicazione

Bookmark ha adottato un sistema di gestione integrato certificato secondo le norme ISO 9001 e ISO 27001 integrato dai controlli previsti dalle Linee Guida ISO 27017 e ISO 27018 per le seguenti attività:

- "Sviluppo, commercializzazione, assistenza, manutenzione Software in ambito gestionale, erogato in modalità Saas e On Premise relativamente ai processi commerciali del retail in contratti, pricing, promozioni, listini e riordino (software Active Demand), sviluppo risorse umane, sostenibilità, gestione

integrata di obiettivi strategici, struttura organizzativa, processi e progetti, formazione e-learning (software Active Trees), erogazione formazione finanziata ed a mercato (software Wally), processi di post vendita (software Active Post Sale)"

## Principi e Obiettivi del SGI

I **principi** generali a cui attenersi riguardano:

- Focalizzazione sul cliente, impegnandosi a soddisfarne le richieste e massimizzarne la soddisfazione;
- L'impegno nel fornire prodotti e servizi di qualità;
- L'impegno nel garantire la sicurezza delle informazioni preservandone le proprietà fondamentali:
  - Riservatezza delle informazioni o confidenzialità: la proprietà di un'informazione di non essere disponibile o rivelata a individui, entità o processi non autorizzati;
  - Integrità delle informazioni: la proprietà di accuratezza o completezza;
  - Disponibilità delle informazioni: la proprietà di essere accessibile e utilizzabile su richiesta di un'entità autorizzata, entro i tempi previsti;
- L'impegno nel rispetto delle leggi e dei regolamenti vigenti;
- L'impegno nel rispetto delle clausole contrattuali;
- La ricerca e l'impegno nel bilanciamento tra: rischio d'impresa, sostenibilità economica, risultati delle analisi del rischio, politiche e strategie aziendali, dei fornitori e dei clienti, nonché adeguamento al contesto dell'organizzazione e perseguimento del miglioramento continuo;
- Principio del "need to know": le informazioni devono essere accessibili sollo a coloro che ne abbiano necessità e autorizzazione;
- Consapevolezza del SGI nel personale aziendale;
- Gestione del rischio cyber e conformità NIS2: in qualità di soggetto essenziale NIS2, Bookmark adotta misure tecniche e organizzative proporzionate al rischio per proteggere i propri sistemi informativi e di rete, garantire la resilienza operativa e adempiere agli obblighi di notifica degli incidenti significativi allo CSIRT di ACN;
- Controllo e qualifica dei fornitori.

Gli **obiettivi** generali del SGI perseguiti con l'impegno del responsabile designato, sono:

- comprendere le esigenze e le aspettative dei clienti, e lavorare per soddisfarle, superandole ove possibile;
- assicurare che tutti i dipendenti siano consapevoli degli obiettivi del sistema di gestione integrato, siano formati adeguatamente e partecipino attivamente al miglioramento della qualità e della sicurezza delle informazioni;
- assicurare che la politica e gli obiettivi del SGI siano comunicati chiaramente a tutti i livelli dell'organizzazione e alle parti interessate esterne;
- minimizzare il rischio di perdita, corruzione, indisponibilità o diffusione illecita delle informazioni e dei dati propri e dei clienti, con idonee misure tecniche e processi a supporto al fine di preservarne la riservatezza, l'integrità e la disponibilità;
- perfezionare la propria capacità di fornire con regolarità prodotti/servizi sicuri, massimizzando gli obiettivi di business;
- svolgere analisi dei rischi che potrebbero compromettere la qualità e la sicurezza delle informazioni;

- effettuare l'esame delle vulnerabilità e delle minacce associate allo scopo di individuare ed attuare le misure correttive e di sicurezza necessarie;
- rispettare le leggi e le disposizioni vigenti, i requisiti contrattuali, le norme e le procedure aziendali;
- promuovere l'attuazione, comprensione e consapevolezza del SGI all'interno dell'organizzazione;
- conformarsi ai principi e ai controlli stabiliti dalla ISO/IEC 27001 Linee Guida ISO 27017- 27018 e dalla ISO 9001 o altre norme/regolamenti che disciplinano le attività di business in cui opera l'azienda;
- perseguire il miglioramento continuo;
- promuovere e concretizzare le politiche per la sicurezza delle informazioni, con particolare riferimento alla tutela dei dati personali;
- monitorare e dimostrare l'efficacia del proprio sistema di gestione integrato;
- promuovere la cultura della cybersicurezza a tutti i livelli dell'organizzazione, attraverso programmi strutturati di formazione e sensibilizzazione del personale sui rischi cyber e sugli obblighi derivanti dalla normativa NIS2;
- adempiere agli obblighi previsti dalla normativa NIS2, in qualità di soggetto essenziale identificato da ACN, implementando e mantenendo le misure di gestione del rischio di cybersicurezza proporzionate al livello di rischio, alle dimensioni dell'organizzazione e all'impatto potenziale degli incidenti;
- garantire la notifica tempestiva degli incidenti significativi all'ACN, nel rispetto delle scadenze e delle procedure previste dal Decreto NIS e dalle determinazioni dell'Autorità competente;
- garantire la sicurezza della supply chain digitale, verificando che i fornitori e i prestatori di servizi TIC adottino misure di sicurezza adeguate e coerenti con i requisiti NIS2;
- potenziare la capacità di rilevazione, gestione e risposta agli incidenti informatici, anche attraverso la cooperazione con CSIRT Italia e le autorità nazionali competenti.

## Impegno della Direzione

L'Alta Direzione si impegna a perseguire, con i mezzi e le risorse adeguate, gli obiettivi e i principi di questa politica.

Bookmark considera i suoi clienti un patrimonio di elevato valore, e ritiene che la massima soddisfazione degli stessi sul suo operato è condizione imprescindibile per il raggiungimento dei suoi obiettivi di business. Allo stesso modo la sicurezza e la tutela del patrimonio informativo sono elementi fondamentali per l'azienda.

Tutto il personale, nell'ambito delle relative responsabilità, è responsabile dell'attuazione della presente politica con il supporto della Direzione, è inoltre coinvolto nella segnalazione di eventuali incidenti o vulnerabilità riscontrati nel SGI.

## RIESAME

La presente Politica viene riesaminata periodicamente dalla Direzione ed eventualmente aggiornata in caso di cambiamenti significativi che influenzino i sistemi, tenendo conto del contesto della realtà aziendale, delle normative, dei risultati delle analisi periodiche e dei successivi monitoraggi.

Forlì,
Data : 07/07/2026

La Direzione