POLITICA GENERALE PER LA SICUREZZA DELLE INFORMAZIONI

Documento ad uso pubblico di **Systrategy S.r.l.**
con sede in Via Galileo Galilei 47, 20092 Cinisello Balsamo (MI),
C.F. e P. IVA 08201040964

REGISTRO DELLE REVISIONI			
Rev.	**Data**	**Attività**	**A cura di:**
v.2.0	14.10.2025	Aggiornamento post Riesame	Resp. SGSI
v.1.1	08.09.2025	Aggiornamenti ISO sul cambiamento climatico	Comitato Sicurezza
v.1.0	15.07.2025	Prima stesura	Resp. SGSI

SOMMARIO

1. Premessa

1.1. Scopo

La **Politica generale per la Sicurezza delle Informazioni** di **Systrategy S.r.l.** definisce l'approccio adottato dall'Organizzazione per garantire la protezione delle informazioni trattate, in conformità con i principi di **riservatezza, integrità e disponibilità**.

Essa costituisce il quadro di riferimento per l'attuazione del **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** e fornisce il riferimento per la definizione e il monitoraggio degli obiettivi di sicurezza.

La Politica recepisce inoltre i requisiti emergenti legati al cambiamento climatico e alla sostenibilità digitale, in coerenza con gli aggiornamenti ISO/IAF, assicurando che tali aspetti siano integrati nelle strategie di sicurezza delle informazioni e di resilienza organizzativa.

Il presente documento è approvato dalla **Direzione**, che ne assicura l'allineamento ai **requisiti normativi e contrattuali applicabili** e ai principi della **ISO/IEC 27001, della normativa in materia di protezione dei dati personali e delle altre norme applicabili in materia di sicurezza delle informazioni**.

1.2. Ambito di applicazione

La presente Politica si applica a tutti i dati e alle informazioni gestite da Systrategy, indipendentemente dal formato, dal livello di classificazione e dalla modalità di trattamento.

In particolare, rientrano nel perimetro di applicazione le informazioni riguardo a:

- **l'Organizzazione e i clienti**, incluse quelle di natura strategica, operativa, finanziaria e tecnica;
- **i dipendenti, i collaboratori, i fornitori e i partner tecnologici** che accedono, elaborano o trasmettono informazioni aziendali nell'ambito delle loro attività;
- **le infrastrutture IT, i sistemi informativi e i servizi cloud** utilizzati da Systrategy, compresi i sistemi *on-premise* e le piattaforme esterne adottate per l'erogazione dei servizi;
- **i processi aziendali**, compresi quelli di sviluppo, gestione e manutenzione di soluzioni IT, trattamento dei dati dei clienti e gestione delle terze parti.

La Politica è parte integrante del **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** di Systrategy e costituisce il riferimento per l'adozione di politiche specifiche in materia di sicurezza.

***

2. Principi fondamentali della Sicurezza delle Informazioni

2.1. Principi	Systrategy adotta un approccio alla sicurezza delle informazioni basato sull'analisi e gestione del rischio, e garantisce che le misure adottate siano proporzionate alle minacce individuate e adeguate agli obiettivi aziendali. La sicurezza delle informazioni è parte integrante della governance aziendale e viene attuata attraverso i seguenti principi: ● sicurezza delle informazioni come **elemento centrale nella gestione operativa, nei processi decisionali e nello sviluppo dei servizi** offerti da Systrategy, con particolare attenzione ai servizi cloud e IT; ● rispetto della **ISO/IEC 27001, del GDPR, delle altre norme in materia di sicurezza delle informazioni** e delle clausole contrattuali sottoscritte con clienti e fornitori, attraverso controlli interni e audit periodici; ● **adozione di misure organizzative e tecniche** per tutelare i dati gestiti, garantendo la riservatezza, l'integrità e la disponibilità delle informazioni attraverso soluzioni di sicurezza avanzate, gestione degli accessi e monitoraggio delle infrastrutture IT; ● utilizzo di strumenti di **monitoraggio continuo** degli eventi di sicurezza e procedure di **Incident Response** per minimizzare l'impatto di eventi critici sulla propria operatività e sui servizi erogati; ● coinvolgimento del personale attraverso **programmi di formazione, simulazioni di attacchi informatici** e procedure operative, **revisioni periodiche e aggiornamenti** in base all'evoluzione delle minacce, dei requisiti normativi e delle esigenze aziendali.
2.2. Obiettivi della Sicurezza delle Informazioni	La presente Politica stabilisce il quadro di riferimento per la definizione dei seguenti **Obiettivi di sicurezza delle informazioni**: 1. **garantire la protezione delle informazioni aziendali e dei clienti;** 2. **migliorare la resilienza operativa e continuità del servizio;** 3. **assicurare la conformità normativa e contrattuale;** 4. **rafforzare la trasparenza e la fiducia nelle relazioni con clienti e stakeholder.** Gli obiettivi di sicurezza sono periodicamente riesaminati per garantirne l'efficacia e l'adeguatezza rispetto all'evoluzione del contesto aziendale, normativo e tecnologico.

***

3. Struttura e applicazione della Sicurezza delle Informazioni

3.1. Ruoli e responsabilità	La sicurezza delle informazioni è una responsabilità distribuita a più livelli all'interno di **Systrategy**, con ruoli definiti per garantire l'efficace attuazione delle misure di protezione e la conformità ai requisiti normativi e contrattuali. **In particolare:** ● **la Direzione** ha la responsabilità ultima del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI), approva la politica di sicurezza, assegna le risorse necessarie, definisce gli obiettivi strategici e approva i risultati del riesame, assicurando che la sicurezza delle informazioni sia integrata nella gestione complessiva dell'Organizzazione; ● il **Comitato per la Sicurezza delle Informazioni** svolge un ruolo di supervisione strategica, supportando la Direzione nella definizione e nel riesame delle politiche di sicurezza, nella valutazione dei rischi e nel monitoraggio dell'efficacia del SGSI; ● il **Responsabile del SGSI** coordina operativamente l'attuazione, il mantenimento e il miglioramento continuo del Sistema di Gestione, garantendo la conformità normativa e il raggiungimento degli obiettivi di sicurezza; ● i **Responsabili di Funzione** integrano la sicurezza nei processi di propria competenza, attuando le misure operative e i controlli previsti dal SGSI per la protezione delle informazioni e dei sistemi sotto la loro gestione; ● il **Personale** ha l'obbligo di conoscere e rispettare le policy di sicurezza, partecipare ai programmi di formazione e contribuire attivamente alla protezione del patrimonio informativo aziendale, segnalando eventuali anomalie o incidenti.
3.2. Struttura delle Politiche di Sicurezza	La **Politica di Sicurezza delle Informazioni** è affiancata da una serie di **politiche e procedure specifiche**, che disciplinano in modo dettagliato i principali ambiti di sicurezza e forniscono linee guida operative per il personale. Le politiche di sicurezza sono articolate nelle seguenti aree: ● **Gestione degli asset** – identificazione, classificazione, protezione e responsabilità sugli asset aziendali; ● **Classificazione e gestione delle informazioni** – definizione dei livelli di sensibilità e delle misure di protezione; ● **Controllo degli accessi** – gestione delle credenziali, autenticazione, segregazione dei privilegi; ● **Gestione dei fornitori** – requisiti di sicurezza per terze parti e gestione dei rapporti contrattuali; ● **Gestione degli incidenti di sicurezza** – processi di rilevamento, risposta e mitigazione; ● **Continuità operativa e backup** – strategie di disaster recovery e test di ripristino; ● **Gestione del personale** – ruoli e responsabilità, formazione e consapevolezza sulla sicurezza;

	● **Sicurezza fisica e ambientale** – protezione degli ambienti aziendali, accessi fisici e videosorveglianza; ● **Sicurezza dei sistemi IT** – protezione delle infrastrutture, gestione delle vulnerabilità e monitoraggio; ● **Sviluppo sicuro** – integrazione della sicurezza nel ciclo di vita del software. Questi documenti vengono riesaminati periodicamente per garantirne la coerenza con la policy generale e con l'evoluzione del contesto normativo, tecnologico e operativo.

***

4. Revisione, aggiornamento e comunicazione	
4.1. Revisione e aggiornamento della Politica	La **Politica di Sicurezza delle Informazioni** e gli altri documenti del SGSI vengono riesaminati con cadenza almeno annuale o in presenza di eventi che possano incidere sulla sua efficacia e adeguatezza. In particolare, la revisione è prevista nei seguenti casi: ● **modifiche normative, regolamentari o contrattuali** che introducano nuovi requisiti in materia di sicurezza delle informazioni; ● **evoluzione del panorama delle minacce** o individuazione di vulnerabilità che richiedano un adeguamento delle misure di protezione; ● **risultati di audit interni o esterni** che evidenzino criticità o opportunità di miglioramento del sistema di sicurezza; ● **incidenti di sicurezza significativi**, la cui analisi renda necessario un aggiornamento delle policy e dei controlli implementati. Le revisioni vengono condotte in coordinamento con le funzioni aziendali preposte e con il **Comitato per la Sicurezza delle Informazioni**. Le eventuali modifiche devono essere approvate dalla **Direzione**, che ne assicura la coerenza con la strategia aziendale e con il **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)**. La revisione periodica tiene conto anche dell'evoluzione dei requisiti ISO/IAF relativi al cambiamento climatico e delle pratiche emergenti di sostenibilità digitale.
4.2. Comunicazione e diffusione	La **Politica di Sicurezza delle Informazioni** è un documento ufficiale dell'Organizzazione e viene reso disponibile a tutte le parti interessate. A tale scopo, Systrategy adotta le seguenti misure: ● la Politica è conservata all'interno del **SGSI**, accessibile al personale autorizzato secondo i criteri di classificazione delle informazioni aziendali;

	● il contenuto dei documenti del SGSI è diffuso attraverso sessioni di formazione periodiche, strumenti digitali aziendali e programmi di sensibilizzazione sulla sicurezza; ● ove applicabile, le politiche specifiche possono essere rese disponibile a clienti, fornitori e partner, con adeguate misure di protezione per evitare divulgazioni non autorizzate; ● i dipendenti e i fornitori che trattano informazioni aziendali devono confermare di aver preso visione della Politica e di rispettarne le disposizioni, attraverso procedure di accettazione documentata. Queste misure garantiscono che la documentazione del SGSI sia sempre aggiornata, conforme ai requisiti applicabili e correttamente recepita da tutti i soggetti coinvolti nella gestione della sicurezza delle informazioni.

***

5. Monitoraggio e conformità	
5.1. Verifica dell'applicazione	Systrategy assicura il rispetto del **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** attraverso un sistema strutturato di monitoraggio e controllo, volto a garantire l'efficacia delle misure di sicurezza adottate e l'adeguamento continuo ai requisiti aziendali, normativi e contrattuali. Le attività di verifica includono: ● **audit interni** (ed eventualmente anche esterni), eseguiti con periodicità definita per valutare il livello di conformità della gestione della sicurezza rispetto agli standard normativi e ai controlli implementati; ● **raccolta e analisi dei feedback** da parte del personale e delle parti interessate, al fine di individuare eventuali criticità, ottimizzare i processi e migliorare l'efficacia complessiva delle misure di sicurezza adottate.
5.2. Adeguamento normativo	La documentazione del **Sistema di Gestione per la Sicurezza delle Informazioni (SGSI)** è sottoposta a un processo di revisione continua, che tiene conto delle evoluzioni normative, dei cambiamenti contrattuali e dell'emergere di nuove minacce. L'adeguamento del **SGSI** avviene in base a: ● **modifiche alle normative e ai regolamenti applicabili** (es. GDPR, NIS2, ISO/IEC 27001); ● **aggiornamenti contrattuali con clienti e fornitori**, con particolare attenzione alle clausole relative alla protezione dei dati e alla gestione della sicurezza;

	● **evoluzione del panorama delle minacce**, incluse nuove tecniche di attacco e vulnerabilità emergenti; ● **esiti di audit, revisioni della direzione e analisi post-incidenti**, che possono evidenziare la necessità di introdurre o rafforzare misure di sicurezza specifiche. Le modifiche alla Politica sono approvate dalla **Direzione**, che ne garantisce la coerenza con gli obiettivi aziendali e le esigenze operative. L'implementazione degli aggiornamenti è affidata al **Comitato per la Sicurezza delle Informazioni**.