Politica per la Sicurezza delle Informazioni

Revisione	Data Revisione	Descrizione	Redatto	Approvato	Classificazione
01	17/12/2025	Prima Emissione	01/12/2025	02/12/2025	Pubblico

Sommario

1. Obiettivi

La Società mette in pratica questi principi con i seguenti obiettivi:

1. Proteggere gli asset informativi aziendali e dei clienti/fornitori acquisiti, trattati o generati nell'ambito dei servizi erogati, salvaguardando la loro riservatezza, l'integrità, disponibilità ed autenticità;
2. Garantire il corretto accesso ai giusti asset informativi quando necessario e prevenire l'accesso non autorizzato, sia da parte di chi opera in IdentifAI, sia di chi opera per suo conto;
3. Implementare misure tecniche ed organizzative per ridurre la probabilità e l'impatto degli incidenti informatici, istituendo processi efficaci di monitoraggio, gestione degli eventi e risposta agli incidenti;
4. Definire ruoli e responsabilità interni ed esterni per la sicurezza delle informazioni, in base a specifiche competenze e background professionale;
5. Supportare il personale e i collaboratori con un'adeguata istruzione e formazione per sensibilizzare in materia di sicurezza informatica al fine di minimizzare i rischi, per quanto possibile;
6. Garantire la continuità della sicurezza delle informazioni e dei servizi core in caso di scenario sfavorevole o qualora si concretizzi una minaccia;
7. Assicurare l'adozione del principio di sicurezza sin dalla progettazione (security by design) e per impostazione predefinita (security by default), introducendo specifici requisiti di sicurezza fin dalle fasi di progettazione, sviluppo e acquisizione dei sistemi, garantendo che le configurazioni predefinite riducano al minimo i rischi informatici;
8. Mantenere l'osservanza delle disposizioni contrattuali, legislative e regolamentari, in particolare sulla protezione delle informazioni, tra cui la norma ISO/IEC 27001:2022 e il Regolamento (UE) 2024/2690;
9. Garantire un'idonea custodia delle informazioni Personali di terzi e la loro gestione secondo principi di liceità, proporzionalità e pertinenza.
10. Assicurare il miglioramento continuo del proprio Sistema di Gestione di Sicurezza delle Informazioni, attraverso le azioni correttive scaturite dagli audit (anche tecnici), i Risk Assessment e la normale operatività.

La Società raggiunge gli obiettivi prefissati di sicurezza delle informazioni tramite un approccio di gestione del rischio strutturato e pianificando opportune misure di mitigazione su diversi fronti.

2. La Direzione di IdentifAI Lab S.P.A.

- ✔ è direttamente responsabile dell'attuazione della presente Politica e dell'osservanza della stessa da parte di tutte le parti interessate;

- ✔ condivide i principi e gli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni (SGSI) e ne sostiene pienamente la realizzazione e il mantenimento fornendo le risorse necessarie a tale scopo;

- ✔ si impegna a mantenere e rafforzare costantemente il livello di sicurezza dei propri sistemi informativi e di rete, mediante attività di verifica e revisione regolare delle misure adottate; ad intervalli pianificati e/o al manifestarsi di eventi significativi (quali incidenti, cambiamenti operativi o risultati di audit), saranno aggiornati processi, strumenti e configurazioni al fine di garantire una risposta efficace alle nuove minacce e il continuo allineamento con le migliori pratiche e standard internazionali;

- ✔ fornisce le risorse e la formazione continua necessaria al miglioramento nel tempo del SGSI.
  È direttamente responsabile dell'allocazione delle risorse necessarie - umane, finanziarie, tecnologiche e procedurali - per realizzare le misure di cibersicurezza e sicurezza delle informazioni; ciò comprende personale qualificato, budget dedicati, tecnologie aggiornate, strumenti di monitoraggio e risposta, nonché processi formalizzati per gestire la sicurezza, la formazione periodica e le attività di controllo.

3. Il sistema di gestione della sicurezza delle informazioni (SGSI)

Il SGSI è una struttura organizzata che coordina e documenta tutte le politiche, le procedure e le azioni messe in atto per raggiungere gli obiettivi della sicurezza delle informazioni e allineare la scrivente allo standard ISO 27001:2022. L'ambito del SGSI comprende tutte le attività e i processi riguardanti le attività operative erogate e quelle amministrative e di supporto.

4. Impatto Ambientale

L'Organizzazione riconosce che le attività legate ai sistemi informativi e alle infrastrutture ICT possono avere un impatto ambientale, sia diretto (consumo energetico dei data center, apparecchiature e dispositivi) sia indiretto (ciclo di vita delle apparecchiature, gestione dei rifiuti elettronici, utilizzo di servizi cloud).
In coerenza con i principi di responsabilità sociale e con gli obiettivi di sviluppo sostenibile, l'Organizzazione si impegna a:

- promuovere l'uso efficiente delle risorse energetiche e digitali, integrando criteri di efficienza ambientale nelle scelte tecnologiche;
- adottare pratiche di riuso, riciclo e smaltimento sicuro delle apparecchiature IT in conformità alle normative vigenti;
- favorire soluzioni digitali e di gestione documentale volte a ridurre l'uso di materiali cartacei;
- considerare l'impatto ambientale nelle decisioni relative alla sicurezza delle informazioni, bilanciando efficacia dei controlli con sostenibilità;
- sensibilizzare i dipendenti e collaboratori su comportamenti responsabili nell'uso delle risorse ICT.

Tale approccio è parte integrante dell'impegno complessivo per la sicurezza delle informazioni, contribuendo a garantire non solo la protezione dei dati, ma anche il rispetto dell'ambiente e delle comunità in cui l'Organizzazione opera.

5. Revisione e aggiornamento

Il presente documento è periodicamente soggetto a revisioni ed aggiornamenti per apportare correzioni ed integrazioni o al fine di garantirne l'adeguatezza e l'efficienza in occasione di cambiamenti significativi riguardanti la sicurezza delle informazioni.

Con l'obiettivo della massima trasparenza e collaborazione, la presente politica per la Sicurezza delle Informazioni è comunicata a tutti i dipendenti e resa disponibile a tutte le parti interessate per quanto ritenuto necessario dal Management.