A. & S. Informatica S.r.l.

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI E DEI DATI PERSONALI

1. SCOPO

Lo scopo del presente documento è quello di descrivere i principi generali di gestione della sicurezza di dati ed informazioni definiti dalla **A. & S. INFORMATICA S.R.L.** al fine di soddisfare i requisiti imposti dalla normativa di riferimento applicabile, in particolare sia la ISO/IEC 27001 che il **Regolamento europeo UE 2016/679** concernente la tutela delle persone fisiche con riguardo al trattamento dati personale e la libera circolazione di tali dati.

2. DESCRIZIONE PRINCIPI E CAMPO DI APPLICAZIONE

La **A. & S. INFORMATICA S.R.L.** al fine di assicurare la sicurezza di dati ed informazioni trattati, sulla base dell'analisi dei processi e delle risorse coinvolte, nonché degli impatti delle attività aziendali sulla sicurezza dei dati gestiti, ha progettato, implementato e mantiene attivo il proprio sistema di gestione sicura, che si applica a tutte le attività economiche d'impresa di seguito sintetizzate:
Progettazione e sviluppo di software. Progettazione, installazione, cablaggio e configurazione di reti locali. Assistenza e manutenzione hardware e software. Commercializzazione ed installazione di apparecchiature hardware. Servizi di consulenza e assistenza informatica.
I principi generali a cui si ispira la Politica aziendale del sistema di gestione sono:

1. Liceità: assicurare che esista sempre un fondamento lecito/giuridico per il trattamento di dati personali;
2. Riservatezza: assicurare che dati ed informazioni siano accessibili solamente ai soggetti e/o ai processi debitamente autorizzati;
3. Integrità: salvaguardare la consistenza di dati ed informazioni da modifiche non autorizzate o accidentali;
4. Controllo: assicurare che la gestione dei dati avvenga sempre attraverso processi e strumenti sicuri e testati;
5. Autenticità: garantire una provenienza affidabile di dati e informazioni;
6. Trasparenza: garantire informazioni coerenti ed aggiornate su responsabili, destinatari e procedure interne definite per la gestione sicura di dati e informazioni.

Nell'ambito della gestione dei servizi offerti la **A. & S. INFORMATICA S.R.L.**, attraverso l'implementazione del Sistema di Gestione per la Sicurezza di dati ed informazioni, assicura:

- la garanzia di aver incaricato un partner affidabile al trattamento del proprio patrimonio informativo;
- il miglioramento dell'immagine aziendale;
- la completa osservanza delle Service Level Agreement stabilite con clienti e fornitori;
- la soddisfazione del cliente, interno ed esterno;
- il rispetto delle normative vigenti e degli standard internazionali di sicurezza.

3. POLITICA PER LA SICUREZZA – FINALITÀ E OBIETTIVI GENERALI

La Politica per la sicurezza della **A. & S. INFORMATICA S.R.L.** rappresenta l'impegno dell'organizzazione nei confronti di dipendenti, clienti e terze parti a garantire la conformità aziendale non solo ai requisiti di legge imposti a protezione dei dati personali, ma anche alle regole interne stabilite dalla Direzione Referente del trattamento dati.

La Politica per la sicurezza si applica a tutti i processi aziendali e persegue le seguenti finalità:

a. Garantire all'organizzazione la piena conoscenza delle informazioni gestite e la valutazione della loro criticità, al fine di agevolare l'implementazione degli adeguati livelli di protezione.

b. Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari.

c. Garantire che l'organizzazione e le terze parti collaborino al trattamento di dati ed informazioni, adottando procedure volte al rispetto di adeguati livelli di protezione e sicurezza.

d. Garantire che l'organizzazione e le terze parti che collaborano al trattamento di dati e informazioni, abbiano piena consapevolezza delle problematiche, effettive o potenziali, relative alla sicurezza.

e. Garantire che le anomalie e gli incidenti aventi ripercussioni sul sistema informativo e sui livelli di sicurezza aziendale siano tempestivamente riconosciuti e correttamente gestiti attraverso efficienti sistemi di prevenzione, comunicazione e reazione al fine di minimizzare l'impatto sul business e sulla tutela dell'interessato.

f. Garantire che l'accesso alle sedi ed ai singoli locali aziendali avvenga esclusivamente da personale autorizzato, a garanzia della sicurezza delle aree e degli asset presenti.

g. Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti.

h. Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità di dati ed informazioni.

i. Garantire la *business continuity* aziendale e il *disaster recovery*, attraverso l'applicazione di procedure di sicurezza stabilite.

La Politica per la sicurezza dei dati, viene costantemente aggiornata per assicurare il suo continuo miglioramento ed è condivisa sia all'interno dell'organizzazione, che con le terze parti ed i clienti, attraverso specifici canali di comunicazione definiti dalla Direzione aziendale.

4. RESPONSABILITÀ PER L'ATTUAZIONE DELLA POLITICA

La Direzione della **A. & S. INFORMATICA S.R.L.** è Referente del trattamento dati ed, assieme al Responsabile Qualità, è Responsabile del Sistema di gestione per la sicurezza di dati ed informazioni, certificato ISO/IEC 27001, implementato con il coinvolgimento dei diversi responsabili di funzione.

Per la gestione dei dati personali e il rispetto del Regolamento UE 2016/679 l'azienda ha provveduto a incaricare il Responsabile della protezione dei dati interno, che supporta la Direzione nel controllo della corretta ed effettiva applicazione delle procedure definite a tutela dei clienti e del personale.

La stessa Direzione definisce compiti e responsabilità dei vari componenti dell'organizzazione, promuovendo la responsabilizzazione e la consapevolezza di ognuno nel perseguimento degli obiettivi generali per la sicurezza di dati ed informazioni definiti.

La Direzione è inoltre garante della verifica periodica del Sistema e della valutazione di eventuali azioni di integrazione e/o modifica dello stesso e della relativa Politica, al fine di assicurarne l'adeguatezza rispetto a:

- evoluzioni significative del business e delle attività espletate;
- nuove minacce rispetto a quelle considerate nell'attività di analisi del rischio;
- significativi incidenti di sicurezza;
- evoluzione del contesto normativo o legislativo in materia di trattamento sicuro di dati personali e informazioni.