POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

GIOTTO COOPERATIVA SOCIALE, dichiara il proprio impegno a realizzare e mantenere un Sistema di **Gestione per la Sicurezza delle Informazioni** secondo lo standard ISO/IEC 27001 in particolare per le attività relative ai servizi di Contact Center e Back office, **perseguendo i seguenti obiettivi**:

- garantire la massima sicurezza delle informazioni dei clienti in termini di Riservatezza - Integrità - Disponibilità delle stesse
- tutelare i diritti e gli interessi di tutti coloro che interagiscono con l'azienda: i nostri stakeholders
- rispettare, anche attraverso la partecipazione dei propri dipendenti, le leggi e le disposizioni vigenti, i requisiti contrattuali e le procedure in essere, conformandosi ai principi e ai controlli stabiliti dalla ISO/IEC 27001:2022 o altre norme/regolamenti, in particolare le regolamentazioni inerenti i trattamenti dei dati personali e la loro sicurezza
- migliorare con continuità il livello del servizio fornito ai clienti, al fine di rendere sempre più efficiente e sicuro il sistema informativo.

La politica della sicurezza delle informazioni di Giotto Cooperativa Sociale, si basa sui seguenti principi:

- Garantire una chiara definizione di ruoli e responsabilità del personale coinvolto nella gestione della sicurezza informazioni
- 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
- Garantire l'accesso sicuro alle informazioni, in modo da prevenire trattamenti non autorizzati o realizzati senza i diritti necessari
- Garantire che l'organizzazione e le terze parti collaborino al trattamento delle informazioni adottando procedure volte al rispetto di adeguati livelli di sicurezza
- 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
- 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
- Garantire la conformità con i requisiti di legge ed il rispetto degli impegni di sicurezza stabiliti nei contratti con le terze parti
- Garantire la rilevazione di eventi anomali, incidenti e vulnerabilità dei sistemi informativi al fine di rispettare la sicurezza e la disponibilità dei servizi e delle informazioni
- Garantire la business continuity aziendale e il disaster recovery, attraverso l'applicazione di procedure di sicurezza stabilite
- Garantire la formazione del personale, sugli obblighi e le responsabilità di ciascuno nella gestione della sicurezza delle informazioni e delle conseguenze in caso di eventi, dolosi e colposi, relativi all'utilizzazione non autorizzata, modifica o distruzione di informazioni critiche, incoraggiando la cultura e la consapevolezza di proteggere dati e informazioni, garantendo la loro riservatezza, integrità e disponibilità
- Attuare obiettivi di miglioramento continuo sul Sistema di gestione, effettuando attività di controllo, riesame, al fine di poter aggiornare i programmi di sicurezza
- Garantire mezzi e risorse in linea con il progresso, mantenendoli sempre in stato di efficienza.

La Direzione