La società AGT Enterprise considera la sicurezza delle informazioni un fattore irrinunciabile per la protezione del proprio patrimonio informativo, per quello dei suoi clienti e dei clienti di questi ultimi.
Per tale motivo ha implementato un Sistema di Gestione per la Sicurezza delle Informazioni, secondo lo standard UNI CEI EN ISO/IEC 27001:2014, e ha attuato un piano di formazione e comunicazione delle best practice e policy in ambito sicurezza delle informazioni sia a livello interno, sia esterno, facendo conoscere la propria POLITICA per la SICUREZZA delle INFORMAZIONI non solo ai dipendenti, ma anche ai clienti, ai fornitori, ai consulenti e a ogni altra parte interessata.

Per la gestione delle attività legate al sistema di gestione, la Direzione assicura la messa a disposizione di tutte le risorse (di budget, umane e tecniche) necessarie, oltre al suo completo coinvolgimento nell'implementazione e mantenimento del sistema e dei suoi obiettivi, che vengono qui di seguito riportati in via generica e meglio precisati nel **Piano degli Obiettivi** aziendale:

- Diffondere a tutti i livelli aziendali le policy e le best practice nella gestione delle informazioni in sicurezza, secondo quanto indicato nella Norma di riferimento e nelle eventuali clausole contrattuali concordate coi clienti, in ottemperanza ai disposti di legge, sia di settore che generali.
- Creare a tutti i livelli aziendali una cultura del Risk Management (sia nella gestione dei singoli processi, sia nella visione sistemica dell'azienda, con particolare riferimento alla gestione in sicurezza delle informazioni e dati propri e dei Clienti, sia in fase di progettazione sia in fase di sviluppo, sia di implementazione dei sistemi e dei software).
- Assicurare in modo proattivo, attraverso gli opportuni mezzi e risorse, la **Business Continuity** negli scenari di rischio ipotizzati e un efficace ed efficiente presidio della sede e di ciò che è in essa contenuto in termini di asset, personale, dati, informazioni, know how, ecc., senza trascurare gli obblighi e le accortezze necessari alla salute e sicurezza sui luoghi di lavoro. La società si impegna altresì a effettuare azioni volte al miglioramento del proprio sistema di gestione della Business Continuity.
- Mantenere e verificare regolarmente la piena efficienza della area **CED** interna alla sede e delle attrezzature in essa contenuta, sia in termini di efficienza funzionale, sia in termini fisici (umidità, temperatura, ecc), sia in termini di sicurezza (accessi, allarmi, antincendio, ecc) e a verificare la piena efficienza anche delle sale CED decentrate (degli outsourcers).
- Assicurare la riservatezza, correttezza, integrità e disponibilità di tutti i dati gestiti per conto dei propri clienti, anche quando affidati a terzi per conto della società, in rispetto degli accordi contrattuali.

- Attuare con continuità ogni sforzo per applicare i principi dello **sviluppo sicuro**, così come evidenziati dalla Norma di riferimento, rendendo consapevoli dell'importanza di attenervisi tutti gli attori coinvolti nel processo e/o nelle sue singole fasi.
- Favorire il **miglioramento continuo** del sistema gestionale e dei processi aziendali in ottica di sicurezza delle informazioni.
- Prevenire non conformità, reclami e **Incidenti Informatici**, impattanti sulle performances e sulla sicurezza delle informazioni, prevenire Data Breach rilevanti ai fini del GDPR. Saper reagire a ognuna di queste problematiche in tempi brevi e in maniera efficace, attuando le giuste comunicazioni e intervenendo nei tempi dettati dalla legge (nei casi di Data Breach)/dagli obblighi contrattuali.
- Scoraggiare fortemente comportamenti illeciti, dolosi o meno, provenienti da qualsivoglia dipendente o collaboratore, attraverso verifiche, controlli, ecc, oltreché attraverso l'emanazione di regole certe.
- Attuare una particolare attenzione nelle **comunicazioni interne,** con messa a disposizione di opportuni strumenti, in particolare **cartelle condivise con accessi differenziati per competenza,** utili alla diffusione di questa e delle altre policy aziendali, oltreché dei suoi obiettivi, nell'ottica di una condivisione, comprensione e consapevolezza allargata e proficua.

La presente politica si lega fortemente alla programmazione, in un documento strutturato, di **obiettivi per la sicurezza delle Informazioni**. Il grado di raggiungimento di tali obiettivi è verificato periodicamente, anche in occasione dei riesami della Direzione. Tale verifica permette di individuare ed adottare (ove necessario) opportune azioni che garantiscano il miglioramento continuo dell'efficacia dei Sistemi.

Tutto il personale è chiamato ad attenersi scrupolosamente alle disposizioni riportate in questo documento, nelle policy e regolamenti che a esso si legano e in qualsiasi altro documento emesso dalla società in relazione alla Sicurezza delle Informazioni, nelle more del proprio ruolo/mansione, anche in relazione alle indicazioni che sono impartite a ognuno dai/l propri/o responsabili/e di funzione.

Qualora ci si trovi in condizioni particolari, situazioni di scostamento o eccezione, la Direzione stabilisce che il personale si attenga alle indicazioni dei responsabili di funzione e alle procedure specifiche che verranno portate a conoscenza degli attori coinvolti; tali procedure dovranno mantenere sempre comunque alto il focus sui principi generali qui espressi.

Il Legale Rappresentante
BENEDETTO OLIVIERI

Agg.ta al 22.01.22