POLITICA PER LA SICUREZZA DELLE INFORMAZIONI

Introduzione

Across considera la Sicurezza delle Informazioni un aspetto primario per la protezione del proprio business e dei propri clienti. La reputazione aziendale si basa sulla corretta gestione degli asset fisici, informativi e del personale: per preservarla è quindi fondamentale un modello della sicurezza che miri a proteggere i processi e le informazioni da un'ampia gamma di minacce e a minimizzarne l'impatto sulla continuità operativa.

Gli obiettivi del Sistema di Gestione della Sicurezza dell'Informazione di Across sono:

- garantire una protezione dell'informazione adeguata in termini di riservatezza, integrità e disponibilità;
- proteggere l'interesse dei clienti, dei dipendenti e delle terze parti;
- assicurare la conformità alle leggi e ai regolamenti applicabili in materia di trattamento e protezione dell'informazione;
- assicurare un modello strutturale alla protezione dell'informazione e alla gestione dei rischi correlati;
- rispondere in modo efficace alle crescenti minacce ai sistemi informativi nello spazio cibernetico.

Questi obiettivi costituiscono il fondamento per la creazione, l'implementazione, il funzionamento, il monitoraggio, la revisione, la manutenzione e il miglioramento continuo di un efficace sistema di gestione della sicurezza delle informazioni, realizzato in conformità alla norma ISO/IEC 27001:2022.

Politica

L'intento della presente Politica è di assicurare che:

- sia attuato un sistema di gestione per la sicurezza delle informazioni (SGSI) per assicurare la riservatezza, l'integrità e la disponibilità delle informazioni alle parti interessate;
- siano rispettati i requisiti legali e normativi applicabili;
- sia rispettato ove applicabile lo standard PCI DSS per quanto attiene alle informazioni relative ai titolari di carte di pagamento;
- siano predisposti, aggiornati e controllati adeguati piani per la continuità dell'attività aziendale;
- tutto il personale riceva adeguato addestramento sulla sicurezza delle informazioni;
- sia garantita la sicurezza delle informazioni anche nel caso di svolgimento delle attività nella modalità in smart-working.
- le procedure e le linee guida per supportare la presente politica siano rispettate da tutto il personale e dai fornitori (o da altre parti interessate);
- al CIO (Chief Information Officer) siano stati assegnati il ruolo e le responsabilità per sovrintendere alla gestione e al funzionamento delle attività connesse all'implementazione della presente policy;
- tutte le violazioni in materia di sicurezza delle informazioni, reali o sospette, siano riportate al COO ed analizzate;
- tutto il personale preposto sia direttamente responsabile dell'implementazione della presente politica in relazione alle proprie aree di competenza e al proprio ruolo;
- siano adeguatamente valutati i rischi per la sicurezza delle informazioni e regolarmente riesaminati in accordo con le politiche di risk management;
- il SGSI sia sottoposto ad audit periodici che ne assicurano l'efficacia e la conformità;
- la presente politica sia riesaminata e aggiornata quando necessario, o almeno annualmente;

- migliorare in modo continuo la sicurezza delle informazioni garantendo nel contempo l’efficacia e la conformità del SGSI.

Rev. 1.0 - 02.04.2025