Politica per la Sicurezza delle Informazioni

	Rif: ISO/IEC 27 001:22 – A.5.1

Scopo e riferimenti

Il Sistema di Gestione della Sicurezza Informativa (SGSI) definisce le regole di protezione della riservatezza, integrità e disponibilità di tutti i dati critici e delle risorse informative del business della ATTITUDE s.r.l.
Esso si applica al perimetro costituito dalle attività di contact center secondo il seguente scopo:

Progettazione ed erogazione di servizi di contact center, comunicazione e digital marketing.

Tutte le regole aziendali in questo ambito seguono lo standard ISO/IEC 27001 e le linee guida ISO/IEC 27002.
Ad esse si aggiungono le misure previste dal Regolamento Europeo per la protezione dei dati Reg. UE 2016/679 (GDPR) e dalla normativa italiana di recepimento.

Impegno della Direzione

La Direzione aziendale considera la sicurezza delle informazioni un fattore critico per il settore di business nel quale opera ATTITUDE s.r.l. e si impegna attivamente ad intraprendere iniziative e progetti per ridurre i rischi, assicurare l'adempimento contrattuale e normativo e adottare le buone pratiche di settore.
Inoltre, per quanto attiene agli investimenti in hardware e applicazioni software, l'impegno è di adeguarsi agli standard tecnologici più avanzati.

Principi di applicazione

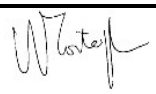
Tutti sono tenuti ad osservare i seguenti principi:

- la sicurezza informativa è dovere e responsabilità di ciascuno, mai il problema di qualcun altro.
- le autorizzazioni di accesso alle informazioni devono essere differenziate in base al ruolo ed agli incarichi ricoperti dai singoli: ogni utente deve poter accedere alle sole informazioni di cui necessita per lo svolgimento delle mansioni ("need to know");
- gli asset aziendali devono essere catalogati e a ciascun asset deve essere assegnato un responsabile ("owner");
- le risorse devono essere utilizzate e protette secondo i relativi requisiti di sicurezza informativa;
- un singolo livello di controlli di sicurezza può rivelarsi insufficiente: un approccio a più livelli deve essere adottato nei casi in cui una perdita di funzionalità ("failure") del sistema informativo sia critico;
- è essenziale studiare, applicare e sottoporre a test le situazioni di utilizzo delle informazioni per assicurare la necessaria capacità di risposta ("response readiness"), continuità del servizio ("business continuity") e ripristino dei servizi critici con danno minimo ("disaster recovery");

ATTITUDE s.r.l. definisce e misura i propri obiettivi specifici di sicurezza informativa, costantemente misurati, verificati e migliorati. Questi devono guidare le decisioni tattiche, così come i principi sopra menzionati guidano le decisioni strategiche.
La Direzione è consapevole che la sicurezza informativa non è assoluta, ma deve essere commisurata al rischio e che il miglioramento continuo è fattore decisivo per mantenere sotto controllo i rischi crescenti e conseguire gli obiettivi di business.

Responsabilità
Tutto il personale interno, collaboratori e fornitori, devono conformarsi a quanto previsto nel presente documento, in quanto inadeguati livelli di sicurezza possono recare danni all'immagine aziendale, comportare insoddisfazione del cliente, generare rischi di incorrere in sanzioni, nonché danni di natura economica e finanziaria.
Chiunque, dipendenti, consulenti o collaboratori esterni, in modo intenzionale o per negligenza disattenda le regole di sicurezza, provocando un danno alla ATTITUDE s.r.l., potrà essere perseguito nelle opportune sedi.
Tutto il personale è responsabile della segnalazione di eventuali anomalie e violazioni di cui dovesse venire a conoscenza.

Riferimenti
- ISO/IEC 27002:2022 "Sicurezza delle informazioni, cybersecurity e protezione della privacy – Controlli di sicurezza"
- UNI CEI EN ISO/IEC 27001:2024 "Sicurezza delle informazioni, cybersecurity e protezione della privacy - Sistemi di gestione per la sicurezza delle informazioni – Requisiti"
- ISO/IEC 27701:2019 "Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines"

Ciclo di emissione	Acronimi	Data	Firma
Redatto da:	NT	04/12/2024	
Verificato da:	AD	24/02/2025	
Approvato da:	GT	24/02/2025	

Rev. N.	Oggetto della revisione	Data
0.1	Draft	04/12/2024
0.2	Approvazione	24/02/2025