

Politica Integrata per la Qualità e la Sicurezza delle Informazioni

Confidentiality - Pubblico (C1)

Revisione	Data	Autore	Stato	Approvato da
04	30/01/2025	RSG	Revisione generale	Direzione
05	30/07/2026	RSG	Integrazione Sicurezza delle informazioni	Direzione

Sommario

1	Scopo	2
2	Campo di applicazione	2
3	Politica integrata per la qualità e la sicurezza delle informazioni.....	2
4	Responsabilità di osservanza e attuazione	3
5	Riesame.....	4
6	Impegno della direzione	4

1 Scopo

La presente Politica stabilisce gli indirizzi e gli impegni di DMT per la gestione integrata della qualità e della sicurezza delle informazioni. In coerenza con la missione, il contesto e gli indirizzi strategici aziendali, i processi sono gestiti secondo i requisiti della norma UNI EN ISO 9001:2015 e della norma ISO/IEC 27001:2022, tenendo conto delle linee guida contenute nella ISO/IEC 27002 nelle rispettive versioni vigenti.

La Direzione definisce, comunica e mantiene attiva la presente Politica a tutti i livelli dell'organizzazione. Essa costituisce il quadro di riferimento per la definizione degli obiettivi del Sistema di Gestione Integrato (SGI) e persegue la capacità di fornire con regolarità servizi conformi ai requisiti dei clienti e alle prescrizioni applicabili, accrescere la soddisfazione delle parti interessate, migliorare continuamente le prestazioni e proteggere le informazioni da minacce interne o esterne, intenzionali o accidentali.

2 Campo di applicazione

La presente Politica si applica a tutti gli organi, i livelli, le sedi, i processi e le risorse dell'Azienda. La sua osservanza è obbligatoria per il personale dipendente, i collaboratori e, per quanto di competenza, per fornitori e soggetti esterni che partecipano all'erogazione dei servizi o trattano informazioni comprese nel campo di applicazione del SGI.

Per la qualità, la Politica riguarda la pianificazione, la commercializzazione, l'erogazione, il controllo e il miglioramento dei servizi. Per la sicurezza delle informazioni, riguarda le informazioni in qualsiasi forma e supporto, nonché i sistemi, le infrastrutture, le apparecchiature e i servizi utilizzati per la loro gestione.

Il campo di applicazione comprende i servizi di telemarketing, customer service e realizzazione di concorsi a premi.

La comunicazione e la diffusione di informazioni verso l'esterno sono consentite esclusivamente per il corretto svolgimento delle attività aziendali, nel rispetto delle autorizzazioni, degli accordi contrattuali, delle procedure interne e delle norme cogenti applicabili.

3 Politica integrata per la qualità e la sicurezza delle informazioni

DMT riconosce che la qualità dei servizi e la sicurezza delle informazioni sono condizioni essenziali per soddisfare i clienti e le altre parti interessate, garantire affidabilità e continuità operativa, tutelare la reputazione aziendale e sostenere nel tempo la redditività dell'organizzazione.

Impegni per la qualità

- porre al centro il cliente, comprendendone i requisiti espressi e, ove pertinenti, le esigenze implicite, e tenere conto delle aspettative delle altre parti interessate rilevanti;
- definire e monitorare obiettivi commerciali, di produzione, del Sistema Qualità e di sicurezza delle informazioni, coerenti con gli indirizzi strategici e misurabili attraverso indicatori appropriati;
- erogare puntualmente i servizi richiesti, assicurando la conformità ai requisiti concordati, standard di servizio definiti, affidabilità e continuità delle prestazioni;
- mettere a disposizione risorse, strumenti e tecnologie adeguati, formalizzandone l'impiego nei processi operativi e cogliendo le opportunità offerte dall'innovazione e dall'evoluzione del mercato;
- mantenere elevati i livelli di competenza, preparazione, formazione e consapevolezza del personale, anche per rispondere a repentini mutamenti degli scenari e degli strumenti tecnologici;
- rispettare i requisiti legali, regolamentari, contrattuali e gli altri requisiti applicabili, gestendo rischi e opportunità e adattando le attività alle nuove necessità dei clienti e delle parti interessate;
- monitorare le prestazioni dei processi e dei servizi, la soddisfazione del cliente, le non conformità e le azioni correttive, promuovendo il miglioramento continuo e il consolidamento del Sistema di Gestione.

Impegni per la sicurezza delle informazioni

Il patrimonio informativo da tutelare è costituito dall'insieme delle informazioni gestite nell'ambito dei servizi e dei processi aziendali, indipendentemente dalla loro forma, ubicazione o modalità di trattamento. L'Azienda assicura:

- la confidenzialità delle informazioni, affinché siano accessibili esclusivamente ai soggetti autorizzati;
- l'integrità delle informazioni e dei metodi di elaborazione, proteggendone accuratezza, completezza e autenticità;
- la disponibilità delle informazioni e dei beni collegati, affinché gli utenti autorizzati possano accedervi nei tempi richiesti dalle esigenze operative.

L'Azienda identifica le esigenze di sicurezza attraverso la valutazione dei rischi, considerando minacce, vulnerabilità, probabilità e conseguenze. I risultati determinano le azioni di trattamento e le misure di sicurezza più idonee, secondo criteri proporzionati alla criticità delle informazioni e dei servizi.

I principi generali di gestione della sicurezza delle informazioni prevedono:

- mantenere aggiornato il catalogo degli asset rilevanti, assegnarne la responsabilità e classificare le informazioni in base alla criticità, applicando livelli di protezione appropriati;
- sottoporre l'accesso ai sistemi a identificazione e autenticazione, attribuendo autorizzazioni coerenti con ruoli e necessità operative e riesaminandole periodicamente;
- definire procedure per l'utilizzo sicuro dei beni, delle informazioni e dei sistemi e diffondere la consapevolezza della sicurezza a partire dalla selezione e per tutta la durata del rapporto di lavoro;
- assicurare la tempestiva segnalazione e gestione degli eventi, delle anomalie e degli incidenti di sicurezza, secondo le procedure definite;
- prevenire accessi fisici non autorizzati alle sedi e ai locali in cui sono gestite informazioni e garantire la protezione delle apparecchiature;
- predisporre misure di continuità operativa e ripristino dei servizi critici, al fine di limitare le conseguenze di eventi imprevisti;
- integrare i requisiti di sicurezza nelle fasi di progettazione, sviluppo, acquisizione, esercizio, manutenzione, assistenza e dismissione di sistemi e servizi;
- garantire il rispetto delle disposizioni di legge, dei regolamenti, degli obblighi contrattuali e degli altri requisiti applicabili alla sicurezza delle informazioni, riducendo il rischio di sanzioni, perdite e danni reputazionali.

4 Responsabilità di osservanza e attuazione

La Direzione approva la presente Politica e garantisce le risorse necessarie per la sua attuazione. L'osservanza e l'applicazione dei principi del Sistema di Gestione Integrato sono responsabilità di:

- Tutto il personale: applicare le procedure, contribuire alla qualità e alla sicurezza dei servizi e segnalare tempestivamente non conformità, reclami, anomalie, vulnerabilità, eventi e violazioni di cui venga a conoscenza;
- I soggetti esterni: rispettare i requisiti contrattuali e le regole applicabili alla qualità dei servizi e alla protezione delle informazioni trattate per conto dell'Azienda;
- Il Responsabile del Sistema di Gestione Integrato (RSGI): coordinare il mantenimento e il miglioramento del SGI, supportare la Direzione nella definizione degli obiettivi, monitorare prestazioni e soddisfazione del cliente, gestire non conformità e azioni correttive, condurre la valutazione dei rischi per la sicurezza delle informazioni, verificare gli incidenti e promuovere formazione e consapevolezza;
- I responsabili di processo: assicurare che i requisiti della presente Politica siano integrati nei processi di competenza e che siano raccolte le evidenze necessarie a valutarne efficacia ed efficienza.

Chiunque, dipendente, consulente o collaboratore esterno, disattenda intenzionalmente o per negligenza le regole stabilite e provochi un danno all'Azienda può essere soggetto ai provvedimenti previsti, nel pieno rispetto dei vincoli di legge e contrattuali.

5 Riesame

La Direzione riesamina periodicamente la presente Politica e, in ogni caso, in occasione di cambiamenti significativi del contesto, dei servizi, delle tecnologie, dei requisiti delle parti interessate o delle prescrizioni applicabili. Il riesame valuta la continua idoneità, adeguatezza ed efficacia del Sistema di Gestione Integrato, considerando almeno il raggiungimento degli obiettivi, le prestazioni dei processi e dei servizi, la soddisfazione del cliente, le non conformità e le azioni correttive, gli incidenti di sicurezza, i rischi e le opportunità, l'adeguatezza delle risorse e le possibilità di miglioramento.

Il RSGI cura il riesame della Politica e ne propone gli aggiornamenti alla Direzione, verificando lo stato delle azioni intraprese e la concreta applicazione degli impegni definiti.

6 Impegno della direzione

La Direzione sostiene attivamente la qualità e la sicurezza delle informazioni mediante un chiaro indirizzo, un impegno evidente, l'assegnazione di responsabilità e l'integrazione del SGI nei processi aziendali. L'impegno della Direzione si attua attraverso le seguenti azioni:

- assicurare che la Politica sia appropriata alle finalità e al contesto dell'Azienda, coerente con gli indirizzi strategici e utilizzata come quadro di riferimento per gli obiettivi;
- promuovere l'orientamento al cliente e garantire il rispetto dei requisiti applicabili ai servizi e alla sicurezza delle informazioni;
- definire obiettivi commerciali, di produzione, di qualità e di sicurezza delle informazioni, monitorandone periodicamente il conseguimento;
- stabilire ruoli, autorità e responsabilità per lo sviluppo, il mantenimento e il miglioramento del Sistema di Gestione Integrato;
- fornire risorse, strumenti, tecnologie e competenze sufficienti alla pianificazione, attuazione, controllo, riesame e miglioramento del SGI;
- assicurare che le procedure e i controlli siano efficacemente integrati nei processi e che le prestazioni e l'affidabilità dei servizi siano monitorate;
- approvare e sostenere le iniziative di miglioramento, le azioni per accrescere la soddisfazione del cliente e le misure di protezione delle informazioni;
- promuovere la formazione, il coinvolgimento e la consapevolezza del personale sui principi della qualità, sulle procedure e sulla cultura della sicurezza delle informazioni;
- assicurare che la Politica sia comunicata, compresa, applicata e sostenuta a tutti i livelli e sia resa disponibile alle parti interessate pertinenti.

Casalecchio di Reno, lì 21 luglio 2026

DMT telemarketing s.r.l. Direzione
MAURIZIO MAESTRI
