

## POLITICA DEL SISTEMA INTEGRATO DELLA QUALITÀ E DELLA SICUREZZA DELLE INFORMAZIONI

WMC è impegnata a mantenere il Sistema di Gestione Integrato conforme ai requisiti delle norme **UNI EN ISO 9001** (qualità) e **ISO IEC 27001:2022** (informazioni), promuovendo una sempre maggiore integrazione nella realtà del sistema di gestione aziendale.

I nostri valori sono:

**PASSIONE:** entusiasmo per i progetti svolti e per il valore che li contengono;

**INNOVAZIONE:** per creare nuove soluzioni, pensando in modo non convenzionale;

**PROFESSIONALITÀ:** Fiducia, lealtà e trasparenza nei rapporti con gli stakeholders;

**ETICA:** rispetto per le persone e per i valori della società in un confronto leale e alla pari;

**ATTENZIONE AL CLIENTE:** essere all'altezza delle aspettative, costruendo relazioni trasparenti con tutti i propri interlocutori;

**SOSTENIBILITÀ:** accogliendo i 17 obiettivi SDGs dell'agenda 2030 dell'ONU e cercando di applicare nella quotidianità azioni che possano soddisfare la loro complessità e trasversalità.

Rilevante quindi nella gestione delle attività e dei progetti sono:

- la soddisfazione dei clienti e di tutte le parti interessate;
- il miglioramento continuo dei processi e dei servizi;
- un lavoro di qualità nel pieno rispetto della Privacy garantendo la tutela della riservatezza, integrità e disponibilità delle informazioni;
- servizi di elevata qualità, sicurezza, diretti a salvaguardare il basso impatto ambientale, continuità e comunicazioni logiche e trasparenti;
- una gestione contrattuale responsabile e trasparente con i fornitori;
- miglioramento continuo del sistema di gestione per la qualità e per la sicurezza delle informazioni;
- coinvolgimento dei partner, creando reti di interesse "culturale" e di business, mettendo a disposizione e acquisendo, a sua volta, esperienze e competenze, in un dialogo continuo.
- rispetto degli obblighi di conformità relativi agli impegni sottoscritti con le parti interessate, ai requisiti cogenti del settore nel quale opera e ai principi delle norme UNI EN ISO 9001:2015 e ISO IEC 27001:2022
- prevenire i rischi alla fonte, cioè in fase di progettazione, scelta dei materiali, individuazione dei metodi e delle tecnologie;
- gestione virtuosa dei rifiuti prodotti, in conformità a quanto stabilito dalla normativa cogente in vigore;
- sensibilizzazione del personale ad adottare comportamenti a basso impatto ambientale negli uffici e di ricerca di soluzioni tecniche che consentano di abbattere i consumi (per es. sensori di luminosità);
- il contenimento dei consumi di combustibile inquinante per gli spostamenti casa/lavoro tramite una pianificazione del lavoro che preveda anche la modalità di lavoro remoto quando possibile e la sponsorizzazione dell'utilizzo di mezzi pubblici;
- assicurare la consapevolezza del personale sugli impatti ambientali e i rischi per la salute e la sicurezza generati dai processi di lavoro e dai comportamenti individuali (fumo attivo e passivo, ecc.);
- promuovendo attività di formazione ed informazione;
- coinvolgimento di tutte le risorse rendendole consapevoli dei loro obblighi individuali e dell'importanza di ogni loro singola azione per il raggiungimento dei risultati attesi e della loro responsabilità.



WMC offre servizi informatici ai propri clienti, appartenenti a tutti i settori di mercato, pubblico e privato. Trattiamo quindi dati pubblici e riservati, dati anonimi, personali comuni e sensibili, dati anche ad alta criticità. Considerando la potenziale criticità dei dati trattati, in qualunque formato essi siano (informatico e non), è fondamentale che sia loro garantita la massima sicurezza. Questo si traduce nella salvaguardia della loro riservatezza in particolare e anche della loro integrità e disponibilità.

I livelli di sicurezza da garantire devono essere tali da rispettare le clausole contrattuali e la normativa vigente, nonché da garantire la coerenza e il bilanciamento tra: rischio di impresa, sostenibilità economica, risultati delle analisi e valutazione dei fornitori e dei clienti, necessità di costante adeguamento al contesto in cui operiamo e di miglioramento dell'efficacia ed efficienza dei nostri processi e di controlli di sicurezza.

I principi cardine a cui attenersi sono:

1. le informazioni devono essere accessibili solo a coloro che ne hanno necessità (principio *need to know*) e nei tempi stabiliti;
2. il personale deve essere opportunamente formato in materia di sicurezza delle informazioni e deve seguire i principi etici e comportamentali prescritti;
- 3, i fornitori devono essere opportunamente tenuti sotto controllo attraverso misure da stabilire a seconda dei casi;
4. i partner devono essere selezionati anche per la loro capacità e disponibilità a conformarsi alle nostre regole di sicurezza;
5. per i servizi erogati, è necessario considerare i requisiti di sicurezza sin dalla contrattazione con il cliente.

**Obiettivi** che l'organizzazione vuole darsi tramite questa Politica Integrata sono attinenti a:

1. Realizzazione di un sistema di gestione che tenga conto delle prescrizioni degli standard e della normativa di riferimento;
2. Attivazione di un Sistema di gestione che costituisca uno stimolo e una guida per il team nell'esercizio delle attività quotidiane;
3. Garantire un sistema di gestione delle informazioni trasparente (in coerenza con le caratteristiche RID) e funzionale ai processi attivati, adottare ed implementare principi e best practice riconosciuti per garantire la Sicurezza delle Informazioni;
4. Individuare ruoli e responsabilità, indipendentemente dal livello gerarchico occupato, coinvolgendo anche i soggetti terzi che svolgono incarichi chiave;
5. Assegnare le risorse necessarie al fine di assicurare l'impiego di misure idonee per gli aspetti riguardanti la sicurezza fisica, logica ed organizzativa;
6. Individuare, documentare ed applicare regole che disciplinano le modalità di utilizzo delle Informazioni, dei beni e degli strumenti;
7. Sviluppare un programma di consapevolezza per il personale, mediante sessioni informative e formative periodiche;
8. Predisporre adeguate misure di reazione e gestione a fronte del verificarsi di incidenti che possono compromettere la sicurezza delle informazioni e la normale operatività;
9. Praticare un confronto leale e valoriale con i mercati con cui si interfaccia in ottica di soddisfazione del cliente e di crescita delle collettività di appartenenza;
10. Ricercare il miglioramento continuo delle performance e del sistema verso una crescita consapevole e adeguata alla business continuity;
11. Tutelare, far crescere e coinvolgere le risorse nel progetto e nella mission aziendale.
12. Creare un sistema di gestione basato su una governance attenta e orientata all'attivazione di scelte sostenibili per se stessa e per la comunità in cui opera.

La responsabilità finale del Sistema Integrato è della Direzione Aziendale che ha delegato i responsabili ad attuare quanto necessario, in accordo con la funzione sistemi IT e il responsabile delle Risorse Umane. Questa politica è comunicata a tutto il personale attraverso i mezzi digitali a disposizione alle parti interessate attraverso la pubblicazione sul nostro sito web.

Elaborato	Approvato
Responsabile del Sistema Integrato: Silvia Fantegrossi	Direzione: Cristiano Verzaro