

Sistema di gestione integrato SGI

ISO 9001 – ISO/IEC 27001 – ISO/IEC 27017 – ISO/IEC 27018 - ISO/IEC 20000-1-  
GDPR

**POLITICA AZIENDALE PER LA QUALITA', PER LA SICUREZZA DELLE INFORMAZIONI E LA GESTIONE DEL SERVIZIO**

PRIMA EMISSIONE

STATO DI REVISIONE – ELABORAZIONE/VERIFICA E APPROVAZIONE					
Edizione 0 Rev. N°	Data	Motivo della revisione	Elaborata da	Verificata da	Approvata da
0	30/06/2020	Prima Emissione	RSGI	AMD L	AMD L
1	22/03/2022	Revisione per recepimento ISO/IEC 27017 e ISO/IEC 27018 e rinnovo della qualificazione AGID	RSGI	AMD L	AMD L
2	30/06/2023	Revisione per adeguamento ISO/IEC 27001:2022 e ISO/IEC 20000-1:2018	RSGI	AMD L	AMD L

*Di seguito viene riportata la politica aziendale per la qualità e per la sicurezza delle informazioni definita dall'Amministratore Delegato in osservanza delle direttive del Consiglio d'Amministrazione e diffusa in azienda affinché tutto il personale ne sia consapevole, ne condivida i principi e si attivi in modo tale da perseguirla. La politica definita viene riesaminata ogni anno, in occasione del Riesame della Direzione al fine di verificarne l'adeguatezza.*

ECOH MEDIA ritiene che la qualità dei prodotti offerti e dei servizi erogati, nonché la cura adeguata della sicurezza e salvaguardia del patrimonio informativo che gestisce, rappresentino asset fondamentali per la soddisfazione dei clienti e costituiscono condizione imprescindibile per il raggiungimento degli obiettivi del business, sui quali basare la propria organizzazione e impostare azioni evolutive di crescita e innovazione. L'azienda è impegnata quotidianamente nel rilevare le esigenze ed aspettative dei clienti e orientare in tal modo le scelte strategiche e operative del proprio sistema organizzativo, nonché nell'implementazione dei requisiti per la sicurezza delle informazioni in modo coerente con gli obiettivi del business e del sistema di gestione integrato.

Il confronto continuo con il mercato ha contribuito alla decisione di sviluppare un Sistema di Gestione Integrato mirato a fornire un prodotto/servizio che fosse il risultato di processi sviluppati in accordo ai criteri stabiliti dalla documentazione di riferimento e da personale competente, in modo da garantire la loro conformità alle aspettative del cliente, ai requisiti normativi e legislativi e alle esigenze di tutti gli stakeholder di riferimento.

Tutto ciò che risulta riferibile alla gestione dei prodotti/ servizi e dei dati merita di essere salvaguardato, difeso e trattato secondo modelli pianificati, accurati e in grado di assicurare la continuità nel tempo delle risorse aziendali.

L'esigenza di dotarsi di un sistema di gestione è legata alla necessità di rispondere prontamente e con efficacia alla globalizzazione dei mercati, all'evoluzione dei sistemi ITC e della tecnologia a supporto e, in particolare, alla necessità di assicurare:

- Efficacia ed efficienza dei processi di realizzazione dei prodotti/servizi, attraverso l'adattamento alle richieste del mercato, l'ottimizzazione dei tempi di gestione, la riduzione dei costi, la minimizzazione degli impatti ambientali, la costante collaborazione con fornitori e collaboratori
- Credibilità, fiducia e confidenza da parte degli stakeholder (ivi compresi i committenti) nel garantire la riservatezza, l'integrità, la disponibilità e la resilienza delle loro informazioni
- Conformità alle leggi, ai regolamenti ed alle direttive che disciplinano le attività di business in cui opera l'organizzazione, con particolare riguardo:
  - ai principi e controlli stabiliti della ISO 9001, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO/IEC 20000-1
  - alle regolamentazioni inerenti la protezione dei dati come il GDPR
- Riduzione dei rischi economici e legali dovuti a perdite di informazioni rilevanti per la continuità del business e per l'interesse degli stakeholder
- Assicurare il rispetto degli SLA di servizio sottoscritti con il cliente in relazione all'erogazione di Servizi IT

- Perseguimento delle opportunità che possano venire a manifestarsi al fine di migliorare la capacità del sistema e la prontezza di risposta alle sollecitazioni del mercato
- Dimostrazione e assicurazione dell'impegno assunto dalla Direzione e da tutti i livelli dell'organizzazione
- La ricerca continua del miglioramento continuo di tutti i processi aziendali, adattandosi

A tal proposito il Sistema di Gestione Integrato:

- si applica alla vendita di prodotti, all'erogazione di servizi, e all'erogazione di applicazioni informatiche in modalità SaaS tramite piattaforme CLOUD
- mira a garantire la comprensione, da parte del personale, delle motivazioni della politica espressa e a far sì che le risorse umane siano consapevoli e partecipi all'implementazione ed al consolidamento del Sistema di Gestione
- salvaguarda la sicurezza delle informazioni, soprattutto quelle ritenute critiche ai fini della protezione dei dati personali e del business aziendale, il che costituisce un elemento essenziale cardine di cui tener conto nell'evoluzione organizzativa futura, facendone uno strumento di cultura imprenditoriale e organizzativa nonché uno dei principi ispiratori della creazione e gestione della conoscenza
- pone come requisito essenziale il rispetto, la valutazione ed il soddisfacimento delle richieste e delle esigenze inesprese del cliente nonché la salvaguardia delle informazioni in merito ad aspetti relativi a:
  - *Riservatezza*: assicurare che l'informazione sia accessibile solo a chi è autorizzato all'accesso
  - *Integrità*: salvaguardare l'accuratezza e la completezza dell'informazione e dei metodi per processarla
  - *Disponibilità*: assicurare che gli utenti autorizzati abbiano accesso all'informazione e agli asset associati quando richiesto
  - *Resilienza*: garantire che i sistemi informativi che trattano il dato abbiano una continuità operativa protesa a fronteggiare le probabili avversità a sistemi e processi conseguenti ad eventi accidentali e/o intenzionali
- è attuato per mezzo di processi che si svolgono all'interno dell'azienda con la collaborazione delle singole funzioni, le cui autorità e responsabilità sono state definite, e dei dipendenti tutti
- mira a garantire l'efficacia di un modello di gestione dei rischi/opportunità aziendali strategici, tattici e operativi strutturato, attraverso il quale il sistema di gestione possa essere stabilito, aggiornato e mantenuto attivo
- è attento a tutti gli aspetti di sicurezza e prevenzione personale
- è attento a tutti gli aspetti inerenti l'ambiente
- è attento a tutti gli aspetti inerenti la privacy, per la cui protezione dei dati personali ha adottato una politica specifica e coerente con la presente
- è documentato in modo da:
  - conseguire la qualità del prodotto/servizio desiderata
  - valutare l'efficacia del sistema stesso

- migliorare la qualità e la sicurezza dei dati
- mantenere e potenziare i miglioramenti
- ottimizza la professionalità delle risorse umane mediante la promozione e la realizzazione di programmi di formazione
- è sostenuto dalla Direzione
- è gestito e diffuso tra i vari enti aziendali dal Responsabile del Sistema Integrato
- è sottoposto, almeno annualmente, a riesame da parte della Direzione onde valutarne l'adeguatezza e l'efficacia
- mira al miglioramento continuo della qualità dei propri processi e dell'immagine aziendale

In relazione alla erogazione di applicazioni informatiche in modalità SaaS tramite piattaforme CLOUD, la Direzione si impegna ad adottare tutti gli opportuni requisiti di sicurezza ed obiettivi di controllo previsti dalla ISO/IEC 27017, con particolare attenzione alla presa in carico dei rischi legati alle attività degli stakeholder che operano per conto dell'organizzazione, alla gestione sicura della infrastruttura, alla gestione degli accessi (con particolare riguardo agli amministratori), alle comunicazioni verso i clienti in occasione di cambiamenti dell'infrastruttura, alla sicurezza dei sistemi di virtualizzazione, alla protezione e l'accesso dei dati dei clienti in ambiente cloud, alla gestione del ciclo di vita degli account cloud dei clienti, alla comunicazione dei data breach e alle linee guida per la condivisione delle informazioni a supporto delle attività di investigazione e forensi, dandone evidenza nella Dichiarazione di applicabilità. Per il servizio di assistenza relativo ai servizi Cloud, la Direzione si impegna ad adottare tutti gli opportuni requisiti di sicurezza ed obiettivi di controllo previsti dalla ISO 20000\_1.

Al fine di assicurare quanto appena espresso, la Direzione intende impegnarsi fattivamente nella definizione di specifici obiettivi di miglioramento del sistema, riferibili direttamente alle strategie identificate e singolarmente riesaminabili in termini di fattibilità e raggiungibilità.

Per raggiungere gli obiettivi indicati, la Direzione si impegna a mettere a disposizione tutti i mezzi e i supporti necessari, quali personale ed infrastrutture idonei, cercando di offrire un ambiente di lavoro che stimoli il miglioramento delle prestazioni aziendali.

L'azienda è consapevole che l'obiettivo della garanzia della qualità dei prodotti/servizi e della sicurezza delle informazioni richiede un impegno costante da parte di tutto il personale operativo e che esso può essere raggiunto con successo solo attraverso un approccio sistematico alle tematiche espresse in questa sede.

La Direzione crede profondamente in questo e si impegna a diffondere e promuovere la consapevolezza dell'importanza della sicurezza delle informazioni all'interno dell'organizzazione.

In occasione del periodico Riesame di Direzione, la Direzione riesamina l'adeguatezza della politica e, ove ritenuto necessario, provvede ad aggiornarla e ad informare i membri dell'organizzazione.