Politica del Sistema di Gestione Integrato per la Sicurezza delle Informazioni, Qualità e Tutela dei Dati Personali

EDIZIONE N° 1		Oggetto	Sigla Responsabili di emissione	
Rev	Data		ELABORATO & VERIFICATO	APPROVATO
			RSGI	DG
0	30.01.2017	Prima emissione documento		
1	30.10.2017	Integrazione Qualità e Sicurezza delle Informazioni		
2	15.01.2020	Integrazione Adempimento GDPR e Protezione dei Dati Personali		
3	29.10.2020	Revisione generale		

Aditinet Consulting SpA

Viale Odone Belluzzi, 57 - 00128 Roma
pi /cf 04137280964 Rea - Roma 1057817
Cap. Soc. € 700.000 i.v.
www.aditinet.it
info@aditinet.it

Milano
Via Torri Bianche, 3
20871 Vimercate (MB)
ph. +39 039 5965582
info@aditinet.it

Roma
Viale Odone Belluzzi, 57
00128 Roma
ph. +39 06 45439252
info@aditinet.it

Northern & Shell Building,
8 th Floor, 10 Lower Thames Street,
London, EC3R 6AF - ph. +44 1189901133
www.aditinet.uk
consultancy@aditinet.uk

Politica della sicurezza delle informazioni, qualità e tutela dei dati personali

Aditinet Consulting è un'azienda di System Integration specializzata in Cybersecurity e Networking in grado di offrire ai propri clienti consulenza specializzata e di realizzare per loro progetti che si basano su soluzioni best of breed, grazie ad una consolidata rete di partnership tecnologiche.

Aditinet mette a disposizione dei clienti tutta la professionalità e la competenza per raggiungere gli obiettivi che questi si sono prefissati. Qualità del servizio, soddisfazione e sicurezza dei dati del cliente sono il centro della nostra azione.

[Società] ha definito le responsabilità per gestire, controllare e attuare tutti i processi relativi al proprio **Sistema di Gestione Integrato (SGI)** relativo alla **Sicurezza delle Informazioni, alla Qualità e alla Tutela dei Dati Personali** in linea con le disposizioni del Regolamento generale sulla protezione dei dati personali (Regolamento UE 2016/679).

L'organizzazione ha l'obiettivo di assicurare la qualità dei servizi erogati e la protezione delle informazioni aziendali e dei dati personali in conformità ai requisiti legali, normativi e contrattuali, tenendo presente i requisiti delle terze parti interessate.

Il suddetto **obiettivo** viene declinato come di seguito specificato:

- **Assegnare** opportuni ruoli e responsabilità per la gestione della sicurezza delle informazioni e la Tutela dei Dati Personali;
- **Proteggere** i Dati Personali di ogni individuo (Protezione);
- **Garantire** l'intimità della sfera personale e della vita privata di ognuno (Riservatezza);
- **Rispettare** l'identità, la personalità e la dignità di ogni essere umano (Individualità e Dignità); nonché il rispetto delle libertà fondamentali costituzionalmente garantite (Tutela).
- **Valutare** periodicamente i rischi di sicurezza delle informazioni e protezione dei Dati Personali al fine di ridurli a livelli accettabili;
- **Aumentare il livello di consapevolezza e competenza** del personale aziendale sugli aspetti relativi alla Sicurezza delle informazioni, alla Qualità e alla Tutela dei Dati Personali;
- **Proteggere il proprio patrimonio informativo** e quello delle parti interessate in termini di Riservatezza, Integrità e Disponibilità;
- **Preservare** al meglio l'immagine aziendale;
- **Evitare ritardi** nell'erogazione dei servizi (rispetto degli SLA);
- **Assicurare e monitorare i requisiti di sicurezza delle informazioni** e di tutela dei dati personali all'interno degli accordi con le parti interessate;
- **Ridurre il numero di incidenti** di sicurezza delle informazioni ed evitare violazioni dei Dati Personali;
- **Soddisfare tutti i requisiti normativi**;
- **Ridurre le vulnerabilità** dei propri asset aziendali da minacce quali virus, software nocivo ecc. tramite interventi di monitoraggio e protezione ad ampio spettro che interessano:

- sistemi hardware e software (personal computer, workstation, server, supporti di memorizzazione, apparecchiature di rete, sistemi di comunicazione elettronica);
- informazioni (banche dati, documenti digitali e dati in transito su sistemi di comunicazione);
- servizi (posta elettronica e accessi al portale).

- **Mantenere** aggiornato ed operativo il Sistema di Gestione della Sicurezza delle Informazioni, Qualità e Tutela dei Dati Personali, conforme rispettivamente allo standard internazionale ISO/IEC 27001:2013, ISO 9001:2015 e al Regolamento UE 2016/679;
- **Sensibilizzare e formare lo staff** sul Sistema di Gestione Integrato (SGI) e sulle sanzioni previste in caso di violazione delle regole;
- **Mantenere la certificazione** di conformità allo standard ISO/IEC 27001:2013 ed ISO 9001:2015.
- **Migliorare continuamente il livello di Sicurezza**, sia "logica" (ad es. attraverso l'analisi per identificare potenziali minacce, garantendo in qualsiasi situazione la disponibilità e la capacità di almeno una copia dei dati per finalità di recovery, riducendo al minimo gli incidenti di sicurezza, aggiornando le patch di sicurezza, ecc.) che "organizzativa" (ad es. attraverso incontri di awareness periodica, training delle nuove risorse, training su nuove policy e procedure, NDA, ecc.).
- **Ridurre** e, per quanto possibile, eliminare le cause di Non Conformità in quanto provocano sprechi e costi aggiuntivi, con possibili danni alla Clientela;
- **Elevare la cultura della qualità** nelle persone che operano in Azienda, rendendole consapevoli dell'importanza del proprio lavoro.
- **Valutare l'efficacia e l'efficienza** del SGI durante i Riesami della Direzione.

Roma, 29 ottobre 2020 **CEO Paolo Marsella**