NUOVA
TECNODELTA S.p.A.
HYDRAULIC PARTS FOR BRAKES AND CLUTCHES
FRAZ. POCOLA, 62 – 14016 TIGLIOLE (AT) ITALIA
TEL. 0141/668111 – FAX 0141/668145

POLITICA PER LA SICUREZZA DELLE INFORMAZIONI (SGSI)

L'azienda ritiene di importanza strategica la protezione delle informazioni e la loro salvaguardia nello sviluppo / realizzazione del prodotto e nel processo produttivo, nonché la riservatezza, l'integrità e la disponibilità dei dati aziendali ed ha deciso di operare affinché gli impianti, i processi produttivi, i servizi, le attività ed i comportamenti non provochino incidenti informatici significativi o generino rischi potenziali / reali per la sicurezza delle informazioni. L'azienda ha organizzato il proprio sistema di gestione sulla base di una conoscenza del contesto in cui opera identificando le parti interessate rilevanti per il suo sistema ed i relativi bisogni ed aspettative rilevanti (obblighi di conformità).

Nuova Tecnodelta ha introdotto nel 2026 il sistema di Gestione per la Sicurezza delle Informazioni secondo la norma UNI CEI EN ISO/IEC 27001.

Il sistema di Gestione per la Sicurezza delle Informazioni ISO 27001 attesta che il sistema di Gestione dell'azienda rispetta le normative cogenti sulla protezione dei dati (incluso il GDPR) ed è orientato ad un miglioramento continuo delle proprie performance in materia di Sicurezza delle Informazioni (inclusa la riduzione delle vulnerabilità e la mitigazione delle minacce informatiche).

L'azienda ritiene fondamentale sotto il profilo strategico e competitivo:

- **il rispetto della normativa in materia di sicurezza delle informazioni e protezione dei dati personali (GDPR / Privacy);**
- **il soddisfacimento della conformità della gestione dei dati e del prodotto ai requisiti cliente / legislazione applicabile;**
- **la prevenzione / riduzione degli incidenti informatici e delle violazioni dei dati (data breach) associabili al proprio prodotto / processo e garantisce la protezione del patrimonio informativo e dei sistemi in un'ottica di continuità operativa;**
- **fornire infrastrutture e accessi tecnologici sicuri per la prevenzione di accessi non autorizzati, perdite o alterazioni di dati correlate al lavoro;**
- **coinvolgere i propri lavoratori e le altre parti interessate nello sviluppo e miglioramento del proprio sistema di gestione (SGSI), considerando tale coinvolgimento e la consapevolezza (awareness) altamente efficaci per il proprio sistema;**
- **il miglioramento continuo delle proprie prestazioni.**

Il Sistema di gestione per la Sicurezza delle Informazioni (SGSI) adottato da Nuova Tecnodelta è adeguato alla natura ed alla scala dei rischi informatici individuati e si propone di migliorare continuamente le proprie prestazioni in campo di sicurezza dei dati ed a controllare le minacce / ridurre i rischi per il patrimonio informativo aziendale andandolo così ad integrare ai sistemi di gestione vigenti che operano in conformità alle norme IATF 16949, ISO 9001, ISO 14001 e ISO 45001.

La presente politica è in linea con il contesto dell'organizzazione, il proprio scopo e la sua dimensione ed è stata sviluppata dalla direzione Nuova Tecnodelta SpA coinvolgendo le funzioni aziendali, tutte le parti interessate/pertinenti e sensibilizzando i lavoratori sui temi della cybersecurity e della protezione dei dati.

NUOVA
TECNODELTA S.p.A.
HYDRAULIC PARTS FOR BRAKES AND CLUTCHES
FRAZ. POCOLA, 62 – 14016 TIGLIOLE (AT) ITALIA
TEL. 0141/668111 – FAX 0141/668145

In relazione a quanto sopra Nuova Tecnodelta:

- **Riconosce che gli obiettivi del Sistema di Gestione per la Sicurezza delle Informazioni hanno importanza pari a quelli di produttività e redditività (integrati nei processi di business ed in linea con l'indirizzo strategico e con il contesto dell'organizzazione) e che la responsabilità del loro raggiungimento è di tutta la struttura organizzativa;**
- **Assicura che le risorse necessarie siano disponibili e che siano all'altezza degli obiettivi del Sistema di gestione (risorse umane, economiche e tecniche, incluse le infrastrutture IT e gli strumenti di cybersecurity);**
- **Considera requisito minimo inderogabile la conformità alle norme di legge in vigore ed agli altri documenti sottoscritti dall'Azienda relativi alle proprie minacce e alla protezione dei dati (incluso il GDPR);**
- **Si impegna ad attuare efficacemente ogni azione volta alla prevenzione degli incidenti informatici, all'eliminazione dei vettori di attacco ed alla riduzione dei rischi per la sicurezza dei dati nonché alla prevenzione delle violazioni (data breach) in tutti i processi nei quali sono svolte attività sotto il proprio controllo, fornendo così un ambiente tecnologico e operativo sicuro;**
- **Si impegna ad attuare il miglioramento continuo dei prodotti, processi, servizi ed attività/comportamenti riducendo, per quanto possibile, le vulnerabilità informatiche, i rischi di indisponibilità dei sistemi e l'impatto sul patrimonio informativo, prevenendo gli incidenti digitali e le situazioni di emergenza (cyber emergency);**
- **Si impegna a razionalizzare, per quanto possibile, l'uso e l'allocazione delle risorse informatiche e degli accessi logici ai dati;**
- **Adotta i programmi a medio e lungo termine necessari alla salvaguardia del patrimonio informativo ed alla riduzione/controllo dei rischi di sicurezza, i quali saranno aggiornati continuamente in relazione allo sviluppo tecnologico, alle nuove minacce informatiche ed alle esperienze maturate;**
- **Assicura che la politica ed il Sistema di Gestione per la Sicurezza delle Informazioni siano continuamente sottoposti a controllo e revisione in ogni loro parte al fine di perseguire obiettivi e traguardi fissati;**
- **Sviluppa, mantiene e controlla un sistema documentale comprese le procedure di gestione degli incidenti e i piani di continuità operativa (Business Continuity e Disaster Recovery);**
- **Promuove la crescita della professionalità / competenze e della sensibilità verso la sicurezza informatica (cyber awareness) del proprio personale e dei terzi con cui opera, attraverso l'informazione e la formazione/addestramento periodico;**
- **Si impegna a consultare e a far partecipare - in ottica proattiva – i propri lavoratori nello sviluppo, pianificazione, attuazione e valutazione delle prestazioni e delle azioni per il miglioramento del proprio sistema di gestione della sicurezza;**
- **Si impegna a individuare ed eliminare gli ostacoli o le barriere alla partecipazione dei lavoratori e ridurre al minimo quelli che non possono essere rimossi, proteggendo i lavoratori dalle ritorsioni dirette o indirette a seguito della segnalazione di incidenti informatici, anomalie di sicurezza, vulnerabilità, rischi e opportunità per la sicurezza delle informazioni;**
- **Informa della presente politica per la sicurezza delle informazioni i fornitori e le imprese appaltatrici, promuovendo una stretta collaborazione al fine di conseguire i migliori risultati in termini di sicurezza della catena di fornitura (supply chain security) e riduzione dei rischi informatici comuni;**
- **Mantiene e promuove rapporti costruttivi di comunicazione con i Clienti, i Partner tecnologici e con le Autorità competenti (es. Garante Privacy, CSIRT o organismi di vigilanza) relativamente alla sicurezza delle informazioni.**

Tigliole, Agosto 2026

ing Massimo Allais
(Amministratore Delegato)