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

INFORMATION SECURITY POLICY

The company considers information protection and safeguards in product development/manufacturing and the production process, as well as the confidentiality, integrity, and availability of corporate data, to be of strategic importance. Consequently, it has resolved to operate in such a manner that its systems, production processes, services, activities, and behaviors do not cause significant information security incidents or generate potential or actual risks to information security. The company has structured its management system based on an understanding of its operating context, identifying the relevant interested parties for its system along with their pertinent needs and expectations (compliance obligations).

In 2026, Nuova Tecnodelta implemented the Information Security Management System in accordance with the UNI CEI EN ISO/IEC 27001 standard.

The ISO 27001 Information Security Management System certifies that the company's Management System complies with mandatory data protection regulations (including GDPR) and is oriented toward the continuous improvement of its Information Security performance (including vulnerability reduction and IT threat mitigation).

From a strategic and competitive standpoint, the company considers the following to be fundamental:

- **Compliance with regulations regarding information security and personal data protection (GDPR / Privacy);**
- **Satisfaction of data and product management compliance relative to customer requirements and applicable legislation;**
- **Prevention and reduction of IT incidents and data breaches associated with its product/process, ensuring the protection of information assets and systems with a view toward operational continuity;**
- **Provision of secure technological infrastructure and access controls to prevent unauthorized access, data loss, or work-related data alterations;**
- **Engagement of its workers and other interested parties in the development and improvement of its Information Security Management System (ISMS), considering such involvement and awareness to be highly effective for its system;**
- **Continuous improvement of its performance.**

The Information Security Management System (ISMS) adopted by Nuova Tecnodelta is appropriate to the nature and scale of the identified cyber risks. It aims to continually improve performance in data security and to control threats and reduce risks to corporate information assets, thereby integrating with existing management systems operating in compliance with IATF 16949, ISO 9001, ISO 14001, and ISO 45001 standards.

This policy aligns with the organization's context, scope, and size. It was developed by Nuova Tecnodelta SpA executive management through the involvement of corporate functions and all relevant interested parties, as well as by raising employee awareness regarding cybersecurity and data protection.

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 relation to the above, Nuova Tecnodelta:

- **Recognizes that Information Security Management System objectives hold equal importance to those of productivity and profitability (integrated into business processes and aligned with strategic direction and organizational context), and that responsibility for achieving them lies across the entire organizational structure;**
- **Ensures that necessary resources are available and adequate for Management System objectives (human, economic, and technical resources, including IT infrastructure and cybersecurity tools);**
- **Considers compliance with applicable laws and other documents executed by the Company regarding threats and data protection (including GDPR) to be a non-negotiable minimum requirement;**
- **Commits to effectively implementing every action aimed at preventing IT incidents, eliminating attack vectors, reducing data security risks, and preventing data breaches across all controlled processes, thereby providing a secure technological and operational environment;**
- **Commits to implementing continuous improvement across products, processes, services, and activities/behaviors by minimizing IT vulnerabilities, system unavailability risks, and impacts on information assets, while preventing digital incidents and emergency situations (cyber emergencies);**
- **Commits to rationalizing, as far as possible, the use and allocation of IT resources and logical access to data;**
- **Adopts necessary medium- and long-term programs to safeguard information assets and control/reduce security risks, updating them continuously relative to technological developments, emerging cyber threats, and lessons learned;**
- **Ensures that the Information Security Policy and Management System are subject to ongoing review and monitoring across all areas to pursue established goals and targets;**
- **Develops, maintains, and monitors a documented system, including incident management procedures and business continuity plans (Business Continuity and Disaster Recovery);**
- **Promotes professional growth, skills, and cyber awareness among its personnel and third parties through information sharing and periodic training/education;**
- **Commits to proactively consulting and engaging workers in the development, planning, implementation, and performance evaluation of security management system actions;**
- **Commits to identifying and eliminating obstacles or barriers to worker participation (minimizing those that cannot be removed) and protecting workers from direct or indirect retaliation following the reporting of IT incidents, security anomalies, vulnerabilities, risks, or opportunities;**
- **Communicates this Information Security Policy to suppliers and contractors, promoting close collaboration to achieve optimum results in supply chain security and shared IT risk reduction;**
- **Maintains and promotes constructive communication with Customers, technology Partners, and competent Authorities (e.g., Data Protection Authority, CSIRT, or supervisory bodies) regarding information security.**

Tigliole, August 2026

ing Massimo Allais
(Chief Executive Officer)