

INTEGRATED QUALITY, ENVIRONMENTAL, OCCUPATIONAL HEALTH AND SAFETY, AND INFORMATION SECURITY POLICY

FRIZONIA Refrigeración-Climatización, S.L. specializes in engineering development, manufacturing, supply and installation of air conditioning and refrigeration systems for application in the industrial, shipbuilding, offshore and defence sectors.

The objective of our Management is to provide high-quality, competitive products and services that meet our customers' contractual requirements, while ensuring compliance with all applicable legal, regulatory and other requirements related to FRIZONIA's activities in the areas of Quality, Environmental Management, Occupational Health and Safety, **and Information Security**, in accordance with the current versions of UNE-EN ISO 9001, UNE-EN ISO 14001, ISO 45001, **ISO 27001** and PECAL 2110. **Furthermore, FRIZONIA is committed to ensuring the confidentiality, integrity and availability of information, while safeguarding the privacy of customers, employees, suppliers and other interested parties.**

Satisfy the needs of clients and stakeholders by maintaining the Integrated Management System through monitoring indicators and risk analysis of the identified processes, defining objectives, taking actions and providing adequate resources to ensure that the services provided are carried out with maximum efficiency, promoting a dynamic of continuous improvement.

FRIZONIA establishes the following principles as a guide and framework in developing its business:

FRIZONIA's commitment to INDUSTRY 4.0 is clear and decisive, leading digital transformation work groups from the R + D + I Area

CUSTOMER COMMITMENT

- ✓ Meeting the needs and expectations of our customers
- ✓ Comply with applicable legal and regulatory requirements
- ✓ Providing the best price/quality relationship of our products and services
- ✓ Establishing professional relationships in a trust environment
- ✓ Meeting agreed deadlines
- ✓ Maintaining data privacy in the whole relationship and project
- ✓ Allow digital, agile, effective and reliable access to the information of the supplied product (CLIENT 4.0)
- ✓ Ensure proper management of market knowledge to offer cutting-edge and innovative products /services.
- ✓ Provide the corresponding security clearance to be able to take part in the contracts/programs or projects in which classified information is to be handled
- ✓ Act with integrity and transparency throughout the activity.
- ✓ To incorporate virtual reality (VR) and augmented reality (AR) tools to improve the customer service quality, adapting to the technological evolution in a way that optimizes the operations and facilitates more efficient and satisfying interactions
- ✓ Implement a strong and effective cybersecurity policy that encourages customer confidence by incorporating additional measures to protect our data, systems, and networks, as well as clear protocols for responding to security incidents and cyberattacks.

COMMITMENT TO STAFF

- ✓ Promoting professional and personal development of our workers through training and awareness programs
- ✓ Encouraging our staff through Participation and Consultation mechanisms for improvement of our integrated system
- ✓ Strengthen Internal Communications to provide information to all staff
- ✓ Improving working conditions in order to raise levels of safety, health and welfare workers
- ✓ Ensuring protection of health and safety of our staff with a permanent goal of reducing accidents and the risk level of our activity

INTEGRATED QUALITY, ENVIRONMENTAL, OCCUPATIONAL HEALTH AND SAFETY, AND INFORMATION SECURITY POLICY

- ✓ Promote the acquisition of new digital skills and competences (TALENT 4.0)
- ✓ Train interested personnel in the concepts of protection of information, classification and its risks, to guarantee the security of that information and request the authorization of personnel who must access to the classified information
- ✓ Following the governing law, protect personal data you have access to while performing your activity
- ✓ To integrate virtual reality (VR) and augmented reality (AR) tools into the workplace to improve operational efficiency and work quality, drive innovation and business competitiveness in a digitalised environment
- ✓ Promote a culture of cybersecurity among staff through regular training, continuous communication, and active engagement, encouraging the establishment of effective practices for protecting the company's information assets and minimizing risks associated with cyber threats.

ENVIRONMENTAL COMMITMENT

- ✓ Promoting actions to avoid pollution
- ✓ Minimizing emissions to atmosphere
- ✓ Promoting Environmentally friendly actions: Reducing, Reusing and Recycling generated waste from our activities
- ✓ Proper Management of generated HTW (Hazardous and Toxic Waste) through authorized managers
- ✓ Using natural resources, raw materials and energy both efficiently and rationally
- ✓ Ensuring compliance with national and international applicable regulations to our field of action
- ✓ Innovating and adapting technological advances in our projects
- ✓ Encourage business digital transformation (COMMUNITY 4.0)
- ✓ Integrate sustainable development criteria in our activities that guarantee an adequate management of resources and protection of the environment.
- ✓ Follow the governing laws in counties in which they are enforced
- ✓ Using artificial intelligence in an ethical and transparent way, ensuring the resulting decisions to be not only efficient, but also fair and respectful with environmental and social principles
- ✓ Integrate the cybersecurity policy into the company's management system to ensure regulatory compliance, establishing greater confidence with clients and business partners, and ensuring the organization's strong commitment to information security.

COMPREHENSIVE RISK MANAGEMENT

- ✓ To provide a greater certainty and security in the achievement of the company's objectives to shareholders, customers, employees and other interested parties, through the anticipation, management and control of the risks of any nature to which Frizonia is exposed with a vision of the whole.
- ✓ Prevent internal and external attacks by implementing cyber-security measures in an integrated manner (CYBER-SECURITY)
- ✓ Eliminate hazards and reduce risks, especially those related to the health and safety at work.
- ✓ Prohibit corruption, bribery and facilitation payment in any form.
- ✓ Predicting and mitigating operational risk using Artificial Intelligence, enabling the organisation to take preventive action before a problem occurs.
- ✓ Define the processes for identifying, analyzing, evaluating, and mitigating detected threats and vulnerabilities that may impact the confidentiality, security, integrity, and availability of the organization's information.

For the purpose of implementing this comprehensive policy, FRIZONIA can rely on competent, involved and committed staff, and from Management, responsibility is assumed in order to have the necessary resources to achieve the scored objectives and goals.

Signed: Management