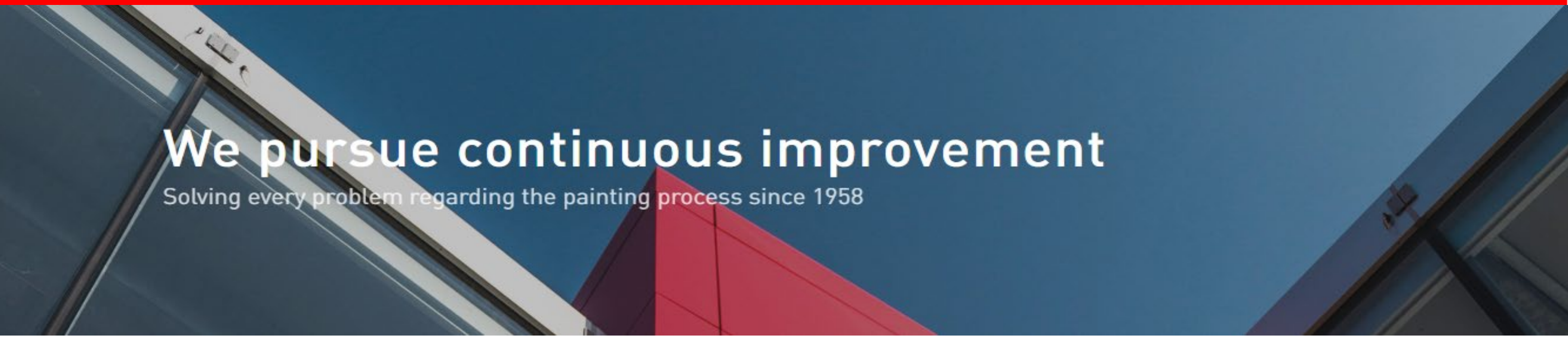
SHOT BLASTING WASHING LIQUID PAINTING POWDER PAINTING CURING

EuroTHERM SINCE 1958
PAINTING INSTALLATIONS



We pursue continuous improvement

Solving every problem regarding the painting process since 1958

CYBER SECURITY DECLARATION

INDEX

1. Declaration of Cyber Security Management

At **Eurotherm S.p.A** we recognize the necessity of maintaining cyber security from the dual perspectives of creating value and managing risk, cyber security measures are a key management priority for our company. We have developed our own Cyber Security Management system; we also promote further enhancement of cyber security measures led by our executive management team in order to address increasingly serious and sophisticated cyber threats including the constant upgrading of our firewalls and other security systems.

2. Recognition of Cyber Security as a Responsibility of Management

The executive management team enhance their own understanding of the latest cyber security circumstances and actively engage in management that positions cyber security spending as an investment. In addition, it takes responsibility for cyber security measures while recognizing that cyber security is a critical management issue, confronting realities, addressing risks, and exercising leadership.

We have positioned measures to address cyberattacks as critical management issue and we promote countermeasures against cyberattacks based on deliberations and validations through executive committees and board meetings to ensure safe and secure financial, personal and technical services are available to our customers.

3. Development of Management Policies and Declaration of Commitment

We aim to provide prompt recovery from security incidents while prioritizing detection, response, and recovery, in addition to identifying and protecting against risks. The executive management team take the lead in declaring the company’s commitment to internal and external partners.

Our internal team and external IT experts perform duties in preparation for cyberattacks during normal times and emergencies. Its duties include cyberattack related information gathering, analysis, and procedures and manual development.

4. Establishment of Internal and External Systems and Implementation of Security Measures

We ensure sufficient resources including budget and personnel, establish internal systems, and take necessary human, technical, and physical measures, as well as developing human resources and conduct training required for those at every level, including management, corporate planning staff, technical specialists, and other employees.

Specifically, we analyse risks of cyberattacks and strive to continuously enhance security and cultivate specialist human resources.

We take measures to evaluate the implementation status of cyber security measures taken within our supply chain, both domestic and international, including our outsourcing partners.

5. Encouragement of widespread use of Cybersafe Products, Systems, and Services

We strive to manage cyber security across the full spectrum of corporate activities, including development, design, production, and supply of products, systems, and services.

Specifically, we take security measures from the time of developing new systems and services to ensure we provide safe and secure services to our customers.

Moreover, we strive to analyze fraudulent transactions and enhance security measures through utilization of one-time password and transaction verification, etc. in internet banking services, etc.

Approved by the Management

Paolo Gluiana

____

Signature and name of a senior executive/CEO representing the company.