

CORPORATE CYBERSECURITY POLICY

TRANSPPOSITION OF DIRECTIVE (EU) 2022/2555 "NIS2" AND LEGISLATIVE DECREE 138/2024

[INTRODUCTION AND REFERENCE LEGISLATION]

Cybersecurity is a key priority for MCE SRL MACHINING CENTERS ENGINEERING. This policy establishes the Management's commitment to adopt a "Cybersecurity Model", aimed at protecting the company's IT systems, as well as the information contained therein, from internal and external threats. In developing the Model, it identifies EU Directive 2022/2555 "NIS2" as the regulatory framework of reference, certifying its full transposition.

[OBJECTIVES]

The adoption of an effective "Cybersecurity Model" pursues the following objectives:
protect your business information from unauthorized access, modification, disclosure or destruction;
ensure business continuity, minimizing risks related to Cybersecurity;
comply with applicable cybersecurity regulations and standards;
contribute to increasing the national and EU level of cybersecurity, to protect society and the market.

[SCOPE OF APPLICATION]

This policy applies to all employees, contractors, suppliers and third parties who access MCE's computer systems and company information.

[CYBERSECURITY PRINCIPLES]

MCE undertakes to adopt appropriate and proportionate technical, operational and organisational measures to manage the risks posed to the security of IT and network systems, used in its business or in the provision of its services, as well as to prevent or minimise the impact of incidents for the recipients of its services. The measures adopted are based on a multi-risk approach, aimed at protecting IT systems and include:
policies for the analysis and treatment of IT security risks;
role management policies and reliability, training, awareness of human resources;
IT critical supply chain management policies;
asset and vulnerability management policies;
business continuity, disaster recovery and crisis management policies;
digital identity, authentication and permission management policies;
data, platform, location, network and communications security policies
security event monitoring and incident management/notification policies.

[RESPONSIBILITY, TRAINING, AWARENESS]

Corporate management: exercises decision-making power in the field of Cybersecurity; assigns roles and responsibilities; approves security measures; supervises their implementation.

IT staff: deals with the implementation, monitoring and updating of IT security measures.

Employees: follow safety policies, procedures, and rules; participate in safety training; report incidents promptly.

Vendors and third parties: They must comply with the same security standards that apply to internal employees and ensure adequate protection measures.

MCE will provide regular training and updates on IT security to all employees, to ensure awareness and understanding of Cybersecurity best practices. MCE will select suppliers who guarantee adequate security standards, periodically monitoring their level of reliability.

[POLICY REVIEW]

The application of this policy will be regularly monitored and possibly supplemented, in the event of significant changes in cyber threats or regulatory requirements. MCE's Management is therefore committed to the

continuous improvement of its Cybersecurity posture, to protect its resources, consolidate the trust of stakeholders and contribute to the development, security and progress of the company.tà.