

Cybersecurity Risk Management Policy

1. Introduction and Regulatory Framework

Cyber security is a key priority for ERCA Group.

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.

This Policy defines the strategic and operational guidelines of the Italian companies belonging to the ERCA Group to ensure a high level of security of networks and information systems, in full compliance with Legislative Decree No. 138 of 4 September 2024 (known as the NIS Decree), which implements EU Directive 2022/2555.

The purpose of this document is to establish principles for risk management and cyber resilience, ensuring business continuity and protection of digital assets.

The main regulatory references governing the Group's compliance are:

- **Legislative Decree No. 138 of 4 September 2024:** Primary regulatory framework on national cybersecurity.
- **Determination of basic obligations (ACN):** Regulates the procedures for compliance with articles 23, 24 and 25 of the decree.
- **Annex 1:** Basic security measures for important subjects.
- **Annex 3:** Types of significant accidents for important subjects.
- **Determination 127434/2026:** Peremptory deadlines for the subjects included in the list starting from 2026.

2. 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

3. Scope

The companies of the group undertake to adopt adequate and proportionate technical, operational and organizational measures to manage the risks posed to the security of the IT and network systems used in their business or in the provision of their services, as well as to prevent or minimize the impact of incidents for the recipients of their services. The measures adopted are based on a multi-risk approach, aimed at protecting IT systems and include:

- policies for risk analysis and security of IT systems;
- incident management plans and threat intelligence sharing;
- business continuity plans;
- encryption policies for the protection of critical and sensitive data, in transit and at rest;

- multi-factor authentication policies for critical access and secure communication procedures in emergency situations;
- security measures in the acquisition, development and maintenance of information systems, including vulnerability management;
- criteria for assessing and managing the risk of critical suppliers.

4. National Cybersecurity Contact

Pursuant to art. 8 of the NIS Decree, the Group identifies an internal National Cybersecurity Contact Person, as a point of contact with the National Cybersecurity Agency (ACN). The Contact Person is responsible for transmitting mandatory communications, coordinating incident notifications and updating personal data on the ACN platform. The name of the Contact Person is formalized in a specific act of the Management and communicated in accordance with the procedures provided for by the ACN.

5. Responsibility, training, awareness

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

The group companies will provide regular training and updates on cybersecurity to all employees, to ensure awareness and understanding of Cybersecurity best practices.

Suppliers will be selected in such a way that they guarantee adequate security standards, periodically monitoring their level of reliability. For critical suppliers, the Group carries out a risk assessment proportionate to the criticality of the service provided and provides, in the relevant contracts, minimum IT security requirements and verification clauses.

6. Policy Review

The application of this policy will be regularly monitored and possibly supplemented, in case of significant changes in cyber threats or regulatory requirements.

The 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.

The Management also periodically assesses the effectiveness of the security measures adopted, including through internal or external verification and audit activities, in order to ensure their adequacy over time with respect to the evolution of threats and regulatory requirements.

Grassobbio, 24/09/2026