Cybersecurity Policy

Cartiere del Garda

April 2026

CARTIERE DEL GARDA recognizes the critical importance of cybersecurity in safeguarding its digital assets, intellectual property, and confidential information. This cybersecurity policy outlines the principles, guidelines, and procedures to ensure the confidentiality, integrity, and availability of information systems and data across all departments and locations of the organization.

1. Objectives

The primary objectives of this cybersecurity policy are:

To establish a framework for identifying, assessing, and mitigating cybersecurity risks.

To protect the confidentiality, integrity, and availability of CARTIERE DEL GARDA's information assets from unauthorized access, disclosure, alteration, or destruction.

To ensure compliance with relevant laws, regulations, and industry standards related to cybersecurity.

To foster a culture of cybersecurity awareness and accountability among all employees, contractors, and partners.

2. Governance and Compliance

The Chief Information Officer (CIO), chairing the Cybersecurity Committee, is responsible for overseeing the implementation of this cybersecurity policy and ensuring compliance with applicable laws, regulations, and industry standards.

Regular reviews and updates of the cybersecurity policy will be conducted to address emerging threats and changes in the business environment.

All employees, contractors, and third-party vendors must adhere to this policy.

3. Risk Management

CARTIERE DEL GARDA will conduct regular risk assessments to identify, prioritize, and mitigate cybersecurity risks across all business functions, locations and IT systems.

Risk mitigation strategies will be implemented based on the identified risks, including technical controls, policies, procedures, and employee training.

4. Access Control

Access to information systems and data will be granted ensuring that employees/third-party partners have only the access necessary to perform their job functions.

Any user is responsible for maintaining the integrity and confidentiality of their credentials to access systems. It is strictly forbidden to share credentials with any other employee or third-party partner.

User access privileges will be reviewed periodically and revoked or modified as needed, especially in cases of employee termination or role changes.

5. Data Protection and Privacy

CARTIERE DEL GARDA is committed to protecting the privacy and confidentiality of personal and sensitive information collected from employees, customers, suppliers and other business partners.

Encryption, access controls, and other appropriate security measures will be implemented to safeguard data both in transit and at rest.

Data retention and disposal policies will be established to ensure the secure disposal of information that is no longer needed.

6. Incident Response and Management

CARTIERE DEL GARDA will develop and maintain an incident response plan (Cyberattack Protocol) to effectively prevent, detect, respond to, contain and mitigate, recover and continuously improve from cybersecurity incidents, including data breaches, malware infections, and denial-of-service attacks.

An incident response team will be designated and trained to handle cybersecurity incidents promptly and efficiently, minimizing the impact on the organization's operations and reputation.

7. Supplier and Third-Party Risk Management

Third-party vendors and suppliers will be evaluated for their cybersecurity practices and adherence to security standards before engaging in business relationships with CARTIERE DEL GARDA. To the same effect, third party vendors and suppliers will be requested to sign the Protocol for accession to Cartiere del Garda's IT systems.

Contracts with third-party vendors will include clauses requiring them to maintain adequate cybersecurity controls and promptly report any security incidents or breaches.

8. Employee Awareness and Training

Regular cybersecurity awareness training will be provided to all employees to educate them about potential threats, security best practices, and their role in protecting CARTIERE DEL GARDA's information assets.

Employees will be encouraged to report any security incidents or suspicious activities promptly to the IT security team.

9. Continuous Improvement

CARTIERE DEL GARDA will continuously monitor and evaluate its cybersecurity posture, conducting periodic audits, assessments, and penetration tests to identify areas for improvement.

Lessons learned from cybersecurity incidents will be documented and used to enhance existing policies, procedures, and controls.

10. Enforcement

Violations of this cybersecurity policy may result in disciplinary action, up to and including termination of employment or contract termination for contractors and third-party vendors.

Employees, contractors, and third-party vendors are required to cooperate fully with investigations into suspected security breaches or policy violations.

The principles set out in this policy shall be implemented and completed by the internal approval of a Cartiere del Garda Cybersecurity Procedure and relevant protocols (use of IT resources, access control, remote working, cyberattack, etc) detailing all the necessary procedures to be followed in each case.