#wearelogistics

Cybersecurity Policy

April 2023

BERGÉ
Moved by Logistics

Index

1. Introduction and subject matter

The purpose of this Cybersecurity Policy (hereinafter the "Policy") is to establish the general principles that apply to the control framework relating to information security, risk management and resilience against cyber security incidents that may affect Bergé Infraestructuras y Servicios Logísticos, S.L. and its subsidiaries (hereinafter "BERGÉ"), as well as to formalise the commitment of the Board of Directors to the implementation, maintenance and improvement of cyber security in the organisation.

BERGÉ considers information and associated systems as important and essential assets for the correct functioning of the organisation and the development of its activity, and therefore assumes cyber security as a responsibility associated with the protection of internal and external threats that may affect these assets in terms of confidentiality, integrity, and availability.

The Policy is aligned with the principles established in the Code of Conduct and other internal policies of BERGÉ and will be complemented with the rest of the procedures, manuals and instructions issued by the Cybersecurity function and the GRC Area.

2. Scope and enforceability

This Policy is addressed to all professionals of BERGÉ and its subsidiaries.

Bergé Infraestructuras y Servicios Logísticos, S.L. and its subsidiaries, subsidiaries understood to be those companies in which Bergé Infraestructuras y Servicios Logísticos, S.L. holds a stake in the share capital that gives it control, in accordance with the provisions of article 42 of the Commercial Code.

The Policy constitutes a binding internal rule for all BERGÉ professionals, regardless of their geographic, hierarchical, or functional location, and regardless of the contractual modality that determines their relationship with BERGÉ.

No general exceptions to the application of the Policy will be approved. If a one-off exception is required for justified reasons, prior authorisation from the CRM Area is necessary.

3. Guiding principles

The following are the general principles and guidelines that should guide BERGÉ's actions in cyber security management:

+ Ensure and communicate cyber security compliance throughout the organisation.
+ Ensure that the information, assets, and systems that support the management of cyber security at BERGÉ have an adequate level of security and resilience, implementing the necessary controls to protect confidentiality, integrity, and availability according to their level of criticality and existing risks.
+ Comply with current legislation, contractual arrangements and regulatory requirements regarding cyber security that are directly or indirectly applicable to BERGÉ.
+ Promote activities to identify, assess and manage identified cyber security risks.
+ Enhance capabilities for prevention, detection, reaction, analysis, recovery, response, investigation and coordination of cyber security incidents and new threats.
+ Establish appropriate cyber security requirements on contractual relations with suppliers and partners.
+ Promote the implementation of appropriate cyber security and resilience mechanisms for assets and systems managed by third parties providing services to BERGÉ.
+ Raise awareness and sensitise all BERGÉ professionals and collaborators to the risks related to cybersecurity and ensure that they have, in an understandable and accessible manner, the knowledge, skills and abilities necessary to identify these risks.
+ Ensure the provision of the necessary material, financial and human resources to meet cyber security-related objectives.
+ Facilitate communication and collaboration with relevant organisations, bodies, government agencies and associations to contribute to the improvement of cyber security in the organisation.

4. Cybersecurity mission at Bergé

The mission of the BERGÉ Cyber Security Department is to protect the company's information assets against cybersecurity threats, developing resilient processes and operations. To this end, the following objectives are set:

- Ensure Cyber Security compliance through the development and implementation of an Information Security Management System.
- Identify, analyse, and manage cybersecurity risks in information assets.
- Advise and accompany affected areas in risk mitigation.
- Establish a culture of cybersecurity in the company, through training and capacity building.
- Provide information to management on the state of cybersecurity (threats, risks, vulnerabilities, and trends).

BERGÉ has a Cyber Security Committee as a Cybersecurity governance body with the following functions:

- Monitoring the progress of the organisation's cybersecurity maturity.
- Review, coordination, and decision-making on cybersecurity incidents.

5. Communication and dissemination

The full text of the Policy shall be made available to all the professionals that make up BERGÉ, all of whom shall be obliged to comply with its content and shall be the object of communication, training and awareness-raising actions for its timely understanding and application.

The Policy will be made available through the corporate Intranet and the organisation's website for promotion to third parties.

6. Approval and review

The Policy was approved by the BERGÉ Board of Directors on 25 April 2023, is incorporated into the internal regulations and may be reviewed and/or modified to adapt to the needs resulting from applicable regulations, technological advances, and other relevant changes in the organisation.

The updating of successive versions of the Policy and/or other documents necessary to comply with its provisions shall be the responsibility of the Cybersecurity Department.