Blulink
VALUE BEYOND COMPLIANCE

Information Security Policy

This policy is aimed to define main objectives and strategic guidelines for Information Security Management System (ISMS) in Blulink organization.

Blulink considers information a precious corporate asset, aimed at supporting the decision-making and processes.
As such, information, including data and their processing, play a fundamental role in the management of activities and the achievement of company objectives.
It follows that Blulink undertakes to identify, collect, process and structure information in a clear, timely, accurate, truthful, complete and secure manner in all business processes in which it is acquired, generated and managed, using a uniform method in order to support the global vision of the company in compliance with applicable laws, standard regulations and interested parties requirements.
The complexity, dynamism, and evolution of the market in which Blulink operates require accurate, rapid and flexible processes. For this reason, it is necessary to have the information available in a secure, timely, effective and efficient manner.

Blulink carries out periodic risk assessments to identify the most suitable measures to guarantee its confidentiality, integrity and availability based on their exposure to identified risks. Risks treatment plans are updated according to new risks and evaluation, exposition and impact changes, and maturity level achieved in both security requirements and controls.

The main purpose is the implementation of an ISMS according to standard ISO/IEC 27001:2022 pursuant the following strategic objectives:

- Secure Software Development Life Cycle of software products and services to make the systems free of vulnerabilities through:
    - adherence to best programming practices and secure coding methods;
    - implementation of security features;
    - continuous security test to detect & fix vulnerabilities;
    - continuous patch delivery.
- Implementation of both technical and organizational measures to assure protection of Customers know-how and confidential information as part of Customers projects documentation of business requirements.
- Reduce occurrence and impact of possible cyberattacks and information security threats towards Blulink infrastructure and assets.
- Respond to interested parties and market expectations.

This document is Blulink property. Unauthorized copy and reproduction are forbidden

- Carry-on of regular risk assessments and definition of risk treatment plans.

- Continuous improvement of ISMS maturity level.

To reach the above listed objectives, Top management has defined roles and responsibilities for information security management. Moreover, external services and synergy with Marposs ICT department have been activated for security and vulnerability management and monitoring.

Blulink intends to pursue its security objectives by referring to the following international standard and regulations:

- ISO / IEC 27001:2022 Information security, cybersecurity and privacy protection Requirements
- ISO / IEC 27002:2022 Information security, cybersecurity and privacy protection Information security controls
- General Data Protection Regulation (GDPR) EU 2016/679

To allow the achievement of the objectives listed in this policy, global guidelines from Marposs (*Information Security Policy*) are the reference point for information security policy in Blulink.

This Policy is distributed to all Blulink organization and is made available through Blulink communication channels to interested stakeholders like Marposs organization, Contractors, Suppliers, Customers, Prospects, Business Partners.

This policy will be reviewed on a two-years cycle basis and updated, as necessary, when and if any major change in Blulink or Marposs organization would arise.

On behalf of Board of Directors
Ing. Bernhard Konzet

Revision	**Date**
00	14/11/2023

This document is Blulink property. Unauthorized copy and reproduction are forbidden