UAB "BALTIC AMADEUS"

INFORMATION SECURITY POLICY

2025-09-19

The purpose of the information security management system maintained by UAB BALTIC AMADEUS (hereinafter referred to as the Company) is to protect the Company's information from various threats, ensuring its confidentiality, integrity, and availability.

INTERESTED PARTIES

When formulating its information security policy, objectives, and control measures, the Company is guided by the needs and expectations of the interested parties. The main interested parties are: customers, employees, business and technology partners, service providers, regulatory and supervisory authorities, the community, and shareholders.

OBJECTIVES

The main objective of this Information Security Policy (hereinafter referred to as the Policy) is to ensure the trust of customers and other interested parties in the Company by guaranteeing the adequacy, sufficiency, and effective functioning of the information security system.

The set of objectives is formulated and implemented with consideration of:

- the Company's strategy and areas of activity;
- requirements set by legislation, contractual obligations, and regulatory authorities;
- the requirements of the ISO/IEC 27001:2022 standard;
- the outcomes of security control implementation and risk assessments;
- lessons learned from information security events and incidents;
- evolving technologies;
- the expectations of clients, employees, partners, and other interested parties;
- management review decisions and audit results.

The Company's information security objectives are set, periodically reviewed, updated as necessary, and their effectiveness is systematically evaluated. The necessary resources are allocated to ensure the achievement of the objectives.

AREAS OF APPLICATION

The Company applies all control measures listed in Annex A of the ISO/IEC 27001:2022 standard as part of its information security management system.

The control measures are adapted to the context of the Company's activities and are implemented to reduce information security risks in all areas of activity. The scope, justification, and implementation procedures for the control measures are documented in separate internal documents related to risk assessment and management. The documents are regularly reviewed and updated to ensure the effectiveness of the system.

RISK MANAGEMENT

The Company applies a formalized information security risk management process, the purpose of which is to identify, assess, and mitigate potential information security threats that could affect the confidentiality, integrity, and availability of information. The results of the risk assessment are documented and used as a basis for the application of information security controls and the improvement of the information security system.

RESPONSIBILITIES

The implementation and maintenance of the information security system is ensured by qualified specialists who are delegated responsibility for the supervision of specific areas.

CONTINUOUS IMPROVEMENT

The company undertakes to continuously improve its information security management system in accordance with the following principles:

- improve the effectiveness of the system in line with best practices;
- ensure compliance with the requirements of the ISO/IEC 27001:2022 standard and maintain certification;
- apply performance measurement and evaluation indicators and adjust actions based on the results;
- encourage employees and other interested parties to submit improvement proposals, evaluate them, and implement them;
- develop expert competencies in the field of information security;
- ensure that documentation is up-to-date, accessible, and understandable.

PRINCIPLES OF OPERATION AND COMMUNICATION

This Policy is published on the Company's website and is available to employees, partners, customers, and other interested parties.

Employees and suppliers must comply with the provisions of this Policy and the documents related to its implementation. If you have any questions about understanding or implementing the requirements, please contact your immediate supervisor or the responsible information security specialist.

REVIEW

The Policy is reviewed at least once a year or when there are significant changes in the Company's activities, risks, legal requirements, applicable standards, or the requirements of customers and other Interested parties.

MANAGEMENT COMMITMENT

This Policy is approved by order of the Chief Executive Officer, and the Company's senior management assumes responsibility for its implementation, maintenance, continuous improvement, and ensures the necessary resources and conditions for the effective operation of the quality management system.

CEO Andžej Šuškevič