INFORMATION SECURITY POLICY

1. GENERAL PROVISIONS

1.1. The purpose of the Information Security Policy is to protect the resources of *DelfinGroup* against external and internal threats and to define the duties and responsibilities of officers and employees.

1.2. The Information Security Policy applies to all employees as well as to third parties using *DelfinGroup* information systems or data.

1.3. The Information Security Policy has been developed in compliance with the legislation of the Republic of Latvia and the ISO/IEC 27001:2022 standard 'Information security, cybersecurity and privacy protection – Information Security Management Systems – Requirements' (hereinafter – ISO 27001 standard).

1.4. The Information Security Management System is part of the integrated management system of the company.

1.5. The Information Security Management System is a set of external and internal legislation, related resources and tools for implementing, maintaining, monitoring and improving information security.

2. INFORMATION SECURITY PRINCIPLES

2.1. *DelfinGroup* ensures that the confidentiality, integrity and availability of resources are maintained in accordance with the established information classification.

2.2. Access to information systems or data is provided on a minimum privilege basis, ensuring that only those accesses are granted that are necessary for the performance of job duties or contractual obligations.

2.3. *DelfinGroup* sets information security objectives and regularly monitors their achievement through operational controls and annual management reviews.

2.4. *DelfinGroup* identifies the information security management requirements applicable to the company, including those arising from laws and regulations and contractual provisions. *DelfinGroup* has assessed compliance with these requirements and is committed to ensuring such in its operations on an ongoing basis.

2.5. *DelfinGroup* ensures the continuous identification and assessment of information security risks in accordance with the Risk management policy in order to mitigate potential threats to the resources of the company.

2.6. *DelfinGroup* ensures that appropriate controls are established and implemented to protect the resources of the company.

2.7. *DelfinGroup* provides the necessary resources and maintains and improves the Information Security Management System in accordance with the strategy, needs and trends of the company.

2.8. Information security principles are followed in internal legislation and contracts.

2.9. *DelfinGroup* ensures that employees are made aware of and comply with the information security system and its requirements, thus ensuring appropriate employee involvement in maintaining information security.

2.10. *DelfinGroup* identifies, records and evaluates events that may affect the information security system.

2.11. *DelfinGroup* provides information security incident management.

2.12. Business continuity is ensured through data backup, regular checking of copies, high availability service for critical systems and a crisis management plan.

2.13. *DelfinGroup* complies with the General Data Protection Regulation and best practices regarding the processing of personal data.

2.14. Security and privacy are integral parts of the *DelfinGroup* project and product life cycle, from planning and implementation to decommissioning.

2.15. *DelfinGroup* supports responsible vulnerability reporting and security research. Security researchers are encouraged to report vulnerabilities by sending an e-mail to netsec@delfingroup.lv, including information that helps to identify the vulnerability.

2.16. The security of the *DelfinGroup* software supply chain is ensured through technical and administrative means and contracts. Components and third-party solutions used in the software are obtained from reliable sources, accounted for and traceable.

3. DUTIES AND RESPONSIBILITIES

3.1. **Supervisory board:**
- 3.1.1. approves the Information Security Policy;
- 3.1.2. provides top-level monitoring of the information security management process.

3.2. **Management board:**
- 3.2.1. takes responsibility for the implementation and enforcement of the Information Security Policy;
- 3.2.2. provides the necessary resources and management support to implement, maintain and improve the Information Security Management System;
- 3.2.3. takes responsibility for the implementation of and compliance with the principles set out in this policy within the Group companies, and the management boards of the Group companies shall ensure the implementation of these principles;
- 3.2.4. takes responsibility for developing and updating the Information Security Policy as necessary, but at least every 3 years.

3.3. **The Internal Auditor** performs internal audits, providing an independent assessment of the internal control system in the area of information security.

3.4. **Responsible Member of the Management board:**
- 3.4.1. oversees the Information Security Management System, its performance and effectiveness;
- 3.4.2. monitors the compliance of the Information Security Policy with the strategy and needs of *DelfinGroup.*

3.5. **Manager of Information System Security:**
- 3.5.1. organises the implementation, maintenance and improvement of the Information Security Management System in accordance with the requirements of the legislation and ISO 27001 standard;

3.5.2. ensures the development and maintenance of documentation related to information security management;
3.5.3. ensures information security risk management (including the coordination of risk assessment, identification of mitigating measures and controls, monitoring of their implementation);
3.5.4. establishes security requirements and monitors their implementation and enforcement;
3.5.5. takes responsibility for incident management.

3.6. **Heads of Units** are responsible for ensuring compliance with the requirements of the Information Security Management System within the Unit.
3.7. **Employees:**
3.7.1. become familiar with and comply with information security requirements in their daily work;
3.7.2. reports identified risks and incidents, as well as cases where information security requirements are not met or cannot be met, to the line manager or the Manager of Information System Security.