# ODİNE SOLUTİONS TEKNOLOJİ TİCARET VE SANAYİ A.Ş.

# INFORMATION SECURITY POLICY

The purpose of the Information Security Policy of our company **Odine Solutions Teknoloji Ticaret ve Sanayi A.Ş. ("the Company")**, is to define the activities required to ensure the confidentiality, integrity and availability of the Company's information systems and information assets, in accordance with all applicable legislation, standards and contractual requirements.

The Information Security Policy applies to all employees who use information and business systems, regardless of their geographical location or business unit, and its implementation is mandatory.

In this context;

**Ensuring Information Security**

- To carry out continuous checks to ensure that all information is accurate and complete, and to minimise information errors and omissions.
- To protect the confidentiality of information and implement effective security measures against unauthorised access. To ensure that only authorised persons have access to information.
- Effectively utilising data backup, secure storage and information lifecycle management practices to ensure the integrity and sustainability of information.
- Ensuring that information is accessible only when necessary and only by authorised personnel.

**Information Security Risk Management**

- Systematically identifying, assessing and managing risks relating to information security.
- To carry out continuous improvement processes by using risk assessment and risk management processes to reduce identified risks to acceptable levels.
- To establish an effective information security risk management approach, identify potential threats and vulnerabilities in advance, and take appropriate measures against them.

**Resource Allocation and Authority Distribution**

- To allocate sufficient human, technological and financial resources for the management of information security risks and the effective operation of security controls.
- To clearly define the necessary authority and responsibilities for information security management and to delegate these to the appropriate individuals.

**Business Continuity and Incident Management**

- To carry out business impact analyses.
- Develop business continuity plans for potential disruptions and emergencies, and test these plans regularly.
- To establish the necessary systems to manage information security breaches effectively and to take appropriate corrective and preventative measures to prevent the recurrence of breaches.

**Service Management**

- Continuously monitor and improve the quality of services provided in accordance with information security policies.

- To define and monitor the service levels committed to customers, and to deliver services in accordance with these levels.

- Ensure service continuity in accordance with information security principles, minimise service interruptions, and draw up backup and recovery plans for emergencies.

- Establishing the necessary procedures to ensure services are delivered securely, and regularly assessing and updating the effectiveness of these procedures.

- To make improvements to service management processes by taking into account customers' feedback regarding information security.

**Compliance with Legislation and Contracts**

- To monitor, understand and fulfil all information security requirements arising from legislation.

- To monitor the information security provisions contained in contracts with business partners, customers and suppliers, and to ensure compliance with these provisions.

**Up-to-Date Business Plans and Procedures**

- To review business plans and procedures regularly and make any necessary updates to ensure they remain up-to-date, practicable and effective.

**Secure Working Environment**

- To raise awareness of information security in order to create a secure working environment for internal and external stakeholders.

- Ensure security in the workplace by implementing physical and digital security measures.

**Information Security Training**

- To provide information security and cyber security training to all staff, and to raise their awareness and understanding of information security.

- To provide the necessary training and information to raise information security awareness amongst third parties and stakeholders.

**Audits and Compliance**

- To carry out regular internal and external audits to ensure compliance with all applicable legislation, standards and contractual requirements.

- To support and monitor planned activities aimed at rectifying any non-conformities that may arise as a result of audits.

**Continuous Improvement**

- To carry out continuous improvement initiatives regarding information security and to develop measures against new threats and vulnerabilities.

- We have set ourselves the objective of continuously improving and keeping the Integrated

Management System up to date with the participation of our staff.

Within the scope of information security, the Company prepares and oversees the implementation of the information security policy and supporting procedures, and establishes mechanisms to ensure that activities related to this policy are carried out.

This Information Security Policy came into force by virtue of Board of Directors' Resolution No. 2024/15 dated 22 July 2024 and is also published on the Company's corporate website. Any amendments to the Information Security Policy shall be subject to the same procedure.

This Information Security Policy has been prepared in both Turkish and English. In case of any discrepancy or inconsistency between the Turkish and English versions, the Turkish version shall prevail. The English translation has been provided solely for the convenience of international stakeholders and does not have legal binding.