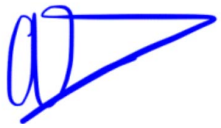
Information Security Policy

Olistek N.V.

History of Changes:

Version	Version Date	Author/Reviewer	Approved By
1.0	15.07.2025	CISO	The Board



Signed By: Andrea Maria Engelhardt - eMagnus Curacao B.V.

Managing Director

Table of Contents

Table of Contents 3
1. GOAL 4
2. SCOPE 5
3. TERMS AND ABBREVIATIONS 6
4. PROVISION OF THE COMPANY'S INFORMATION SECURITY 7
4.1. Information security principles 7
5. ROLES AND RESPONSIBILITIES 8
6. ENFORCEMENT 9
7. INFORMATION SECURITY PRINCIPLES 10
7.1. Efficiency 10
7.2. Continuous Improvement 10
7.3. Visibility and Communication 10
7.4. Segregation of Duties 10
7.5. Role-Based Access Control 10
7.6. Least Privilege 10
7.7. Defense-in-Depth 10
7.8. Ownership and Responsibility 10
7.9. Personal Responsibility 10
7.10. Awareness 11
8. DOCUMENT REVISION 12

1. GOAL

This policy aims to protect the confidentiality, integrity, and availability of information assets, aligning with Olistek N.V. (Hereinafter — «the Company») business objectives and compliance requirements.

2. SCOPE

This Policy applies to all business processes and the Company’s Information Assets, which are used to achieve its business goals. This also includes relationships with business partners, contractors, and providers, with whom the Company's Information Assets are used, including electronic, paper, and physical data carriers.

The requirements of this Policy are obligatory for execution by all Users of Information Assets of the Company.

3. TERMS AND ABBREVIATIONS

Information Asset (hereinafter – Asset) - is information itself or objects that contain, process, store, or transmit information, as well as business operations which support the organization's mission and its continuity.

Information security (IS) is a complex of measures aimed at ensuring the protection of information from unauthorized access, use, disclosure, damage, modification, review, validation, record, or destruction**. The purpose of Information security** is to protect the Information Assets of the Company.

The level of information security is defined by the absence of critical risk associated with the leakage of information through unauthorized channels, technical, and unintentional actions with data used in information systems.

ISMS (Information Security Management System) is a part of the overall risk management system of the Company, which is aimed at creating, implementing, storing, operating, monitoring, reviewing, maintaining, and improving Information Security**.**

The User is a person who uses Information Assets of the Company for the execution of business processes, including employees, contractors, or other third parties who are authorized to use the Assets**.**

Information security incident - breach or suspected breach of established procedures or requirements of the Company in the areas of Information Security and IS risk management.

Asset registry – a list of assets containing details of the persons who are responsible for every Information Asset, determines the level of criticality of the Asset with respect to the availability, confidentiality, and integrity of the information.

4. PROVISION OF THE COMPANY'S INFORMATION SECURITY

4.1. Information security principles

Information security is an integral part of the Company's Information Assets, which in turn are a business-making tool of the Company. Specifically, this policy aims to protect the confidentiality, integrity, and availability of information assets, aligning with the company's business objectives and compliance requirements.

Information security should provide the necessary level of Asset security in line with the Company's objectives.

Information security is provided by carrying out appropriate physical, technical, and administrative measures and measures regulated by local legislation, which are supported by the Company's management in an appropriate manner and on the basis of relevant business processes and procedures.

General principles of Information Security over Assets are**:**

- ***Confidentiality:*** *to ensure non-disclosure of required information to third parties if such information is classified as restricted;*
- ***Integrity:*** *to ensure the accuracy of the information and its completeness;*
- ***Availability:*** *to provide secure access to information at the right time and in the right place.*

Confidentiality, integrity, and availability are the main principles of maintaining the Company's competitiveness, legal compliance, and compliance with the Company's image.

In accordance with the signed NDA, the Company's employees and contractors are prohibited from disclosing or transferring information beyond the "confidential" level, and without an approved business purpose.

The Company's management declares its full support in building information security in the Company and in working with corporate and other parties.

Information security must take into account current and emerging security threats to be able to implement necessary countermeasures and mitigate the risk.

The required level of the Asset's information security is achieved through physical, technical, and administrative controls and actions prescribed by the regulation.

Activities, methods, and practices used for Asset protection should consider the level of economically justified risk and the desired level of the Asset's information security.

Information security is continuously improving, taking into account the objectives of the Company, optimizing IS processes using new security technologies, and improving the effectiveness of existing ones.

Information security communication channels: Slack channels, corporate mail.

5. ROLES AND RESPONSIBILITIES

The Chief Information Security Executive Officer is **responsible** for the implementation, realization, and control of the maintenance of the required level of Information security in the Company.

The Information Security Team is responsible for:

- Coordination of the implementation process of the Information Security Management System in accordance with the requirements of this Policy.
- Control and support of the process of Asset inventory and periodic review of the Asset registry.
- Monitoring and controlling the proper implementation of the requirements of this Policy.
- Coordination and implementation of the IS risk management process and implementation of measures aimed at increasing the level of information security of the respective Asset.
- Training and User consultancy on Information security issues.
- Increase the awareness of employees regarding IS policies and procedures.

The Chief Information Security Executive Officer and the Information Security Team coordinate activities to support Information security as part of a comprehensive security system of the Company**.**

Information Security Policy regulations are developed by the Information Security Team and other departments in the relevant areas of activity. Permanent control over the implementation, execution, improvement, and maintenance of the Policy regulations in an up-to-date state is entrusted to the Information Security Team.

Managers of all levels (functional groups managers, heads of groups, etc.) are personally responsible for Information security in the subordinate units, as well as for compliance with the requirements of the IS for the Assets that are in scope of their responsibility.

Employees and contractors of the Company as Asset Users should be aware of the requirements of the information security policy and must comply with it.

Users of the Assets must:

- Strictly adhere to the Policy and IS requirements.
- Use the Assets only for the business purposes of the Company.
- Accurately and timely inform about known or suspected security incidents in accordance with the Security Incident Management Policy.

6. ENFORCEMENT

Requirements of all ISMS regulations should be reflected in the formal job descriptions of Users.

The relationships of the Company with third parties that require access, processing, supporting, or managing Information Assets of the Company must comply with the current Policy requirements and be a part of contractual agreements between the parties.

The Company's information technology development strategy, all projects related to information technology, should be consistent with the Information Security Policy.

7. INFORMATION SECURITY PRINCIPLES

7.1. Efficiency

Resources allocated to maintain corporate Information Security should be commensurate with the risks of information security.

Efficiency should be a part of the process of measurement and evaluation. Results of the efficiency measurement should be communicated to the CEO and the Board.

7.2. Continuous Improvement

Corporate Information Security is a continuous process within the company that should be constantly reviewed and improved to be compliant with the requirements of legislation, contractual obligations, and standards.

7.3. Visibility and Communication

Security decisions, incident resolutions, plans, and results should be timely and clearly communicated to the required audience, top management, employees, contractors, partners, etc., if it will not harm the company or its interests.

7.4. Segregation of Duties

Conflicting duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the company's assets.

Required security measures on the organizational and technical levels should be implemented to support this principle.

7.5. Role-Based Access Control

Access permissions should be assigned based on predefined roles, streamlining the management of user privileges by associating permissions with specific job functions, positions, and business units.

RBAC should enhance security, simplify administration, and ensure users have the appropriate access rights aligned with their roles within an organization.

7.6. Least Privilege

Access to assets should be provided at a level no higher than necessary to enable the performance of tasks. In other words, the principle of "need-to-know" must be implemented in the access control process, where it's possible.

7.7. Defense-in-Depth

This approach aims to mitigate the impact of security breaches by having multiple lines of defense, including physical, technical, and administrative controls.

Implementing multiple layers of diverse security measures across an organization's infrastructure will allow us to create a robust and comprehensive defense against various potential threats.

7.8. Ownership and Responsibility

All assets, risks, requirements, and controls should be defined, documented, and assigned to their owners. Asset owners are responsible for their protection.

By delineating ownership and responsibilities, we can establish a proactive and accountable security culture that enhances the overall protection of assets and sensitive information.

7.9. Personal Responsibility

All employees and users underscore individual accountability for adhering to security policies, safeguarding sensitive information, and actively participating in maintaining corporate security.

By fostering a culture of personal responsibility, we empower individuals to contribute to a collective effort in fortifying cybersecurity defenses.

7.10. Awareness

All employees and users should be informed about the principles and requirements of information security and should be involved in the corporate security management process.

8. DOCUMENT REVISION

Revision of the provisions of this Policy is performed not less than once in two years or in the case of changes to business objectives or activities of the Company.