KVS-6-5Information Security Policy
Effective Date: 2026-03-16 Version:3
Policy Author: Head of the Information Systems Department
Policy Approved By: *Chief Executive Officer*
Published: Privately ☐ Publicly ☒

1 GENERAL PROVISIONS

1. The Information Security Policy (hereinafter referred to as the Policy) is the primary document establishing the fundamental information security objectives, assurance, and management principles of UAB "Axioma Trade."
2. The Policy applies to all employees, contractors, and third-party suppliers of UAB "Axioma Trade" who have access to the organization's information resources and systems.
3. The policy has been developed in accordance with the requirements of ISO/IEC 27001:2022 "Information Security, Cybersecurity, and Privacy Protection" (hereinafter referred to as ISO 27001) and the network and information system security requirements of the European Union's NIS2 Directive (NIS2, 2022/2555) on the security of network and information systems, and the European Union's Cyber Resilience Act (CRA, 2024/2847) on secure development and vulnerability management.

2 THE OBJECTIVE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

1. To protect all information from all possible threats—external, internal, intentional, or accidental—that could affect the company's operations and reputation.
2. To ensure compliance with information security requirements as stipulated in the laws of the Republic of Lithuania and the ISO 27001 standard.
3. Ensure the implementation of necessary information security management measures.
4. Prevent incidents related to information security breaches that could disrupt the company's operations, or mitigate the potential impact of such incidents.
5. To foster a culture of information security awareness and accountability throughout the organization.

3 INFORMATION SECURITY MANAGEMENT

ISMS helps protect the company's information assets, strengthen its reputation, and achieve business objectives.

3.1 Risk Management

- Risk assessment is performed regularly and whenever significant changes occur within the organization, its operations, or the external environment.
- Senior management establishes risk acceptance criteria and regularly monitors risk assessment and management.

3.2 Data Protection

- Data is classified according to confidentiality criteria, and security measures are established.
- The company is committed to protecting personal and sensitive data in accordance with applicable data protection regulations.
- Transparent data processing activities and the rights of data subjects are ensured.

3.3 Asset Management

- All of the company's most important assets are identified, categorized, and recorded in an asset inventory.
- Each asset is assigned owners who are responsible for its maintenance and protection.

3.4 Incident Management

- A consistent and effective incident management process is applied to manage information security incidents, minimizing potential impact and ensuring timely recovery.
- The established incident response procedure includes classification, prioritization, communication, escalation, and analysis.
- All employees and contractors are required to report any observed or suspected security vulnerabilities or incidents.
- Lessons learned from incidents are evaluated, and the experience gained is used to improve the ISVS.
- Information security incident management processes are aligned with and integrated into the information security incident management of the National Cyber Security Center of the Ministry of National Defense.

3.5 Access Management

- Access to information and system components is granted based on the principles of least privilege and "need-to-know" separation of duties.
- User access is reviewed periodically.
- Procedures for granting, modifying, and revoking access rights are documented and followed.

3.6 Backup and Recovery

- Backups of data critical to the company's operations are made regularly.
- Recovery procedures are tested periodically to ensure the rapid restoration of data and services in the event of a failure.

3.7 Operations and Communications

- To ensure the proper and secure operation of information processing equipment, operational procedures and responsibilities are documented and managed.
- Protection against malware is implemented and maintained on critical systems, and necessary updates and data encryption are ensured.
- Event logs recording user actions, exceptions, failures, and security incidents are generated, stored, and reviewed regularly.

3.8 Secure Development Process

- The company follows a secure software development lifecycle, during which security is integrated into every stage, including the use of static and dynamic code analysis tools and regular training on secure coding practices.
- Separate development, testing, and production environments must be maintained with strict access controls.
- A comprehensive security review must be performed before software deployment.
- An effective feedback mechanism is ensured so that security issues identified after deployment are incorporated into future development. Strict patch management and version control are applied.

3.9 Physical and Environmental Security

- Physical security measures are in place for premises where critical IT systems and classified information or data are stored.

3.10 Business continuity and disaster recovery planning

- The company has a business continuity and recovery plan that takes into account potential threats and operational disruptions.
- This plan is tested and reviewed regularly to ensure its effectiveness in the event of an emergency.

3.11 Relationships with Suppliers

- Information security requirements for suppliers with access to the company's information systems and assets are specified in contracts.
- Suppliers' compliance with information security requirements is assessed periodically.

3.12 Employee training

- Employees receive regular training on information security and data protection.
- Specialized training is provided to individuals performing specific security functions and assuming responsibility.

3.13 Continuous improvement

- The adequacy and effectiveness of the ISMS are improved through risk assessment, effectiveness measurement, internal audit, and an evaluative analysis of ISMS management, including the planning and implementation of corrective actions.

4 VALIDITY AND DOCUMENT MANAGEMENT

1. The information security policy is reviewed at least once a year or following any significant security incident, regulatory changes, or organizational changes.
2. The Information Security Policy is available to all interested parties.
3. All employees are made aware of the Policy and its amendments through the document management system (DMS) or other means.

Permit No.	Date of Preparation	Description of the version	Reason for Issuance	Prepared by (department)
1.	2023-11-20	Document issued	New	Quality Department
2.	March 14, 2024	Document published	Policy provisions (sections 3, 4, 5, 6) have been transferred to the Information Security Management Procedure	Quality Department
3.	March 16, 2026	Additions to the document	Declaration of compliance with EU Directives TIS2 and CRA	Information Systems Department