Approved by:
Šarūnas Matijošaitis, Chairperson of the Board
of Vičiūnai Group
Order No.A25-09-83, 2025-09-24

INFORMATION SECURITY POLICY OF VIČIŪNAI GROUP

TABLE OF CONTENTS

CHRONOLOGY OF POLICY AMENDMENTS			
Amendment No.	Date	Nature of the amendment	Amendment performed by:
1.			

1. PURPOSE

1.1. The **purpose** of the Information Security Policy (hereinafter referred to as **"the Policy"**) is to establish the main information security objectives, management principles, and responsibilities; to ensure the adequacy, effectiveness, and suitability of the information security management system for the strategic objectives of the Vičiūnai Group, and to ensure its maintenance in accordance with operational, legal, statutory, regulatory, and contractual requirements.

1.2. The Vičiūnai Group (hereinafter referred to as "**the Group**") undertakes to ensure the confidentiality, integrity, and availability of information, regardless of the form (a hard or soft copy) in which it is stored, and to protect it against unauthorised use and disclosure.

2. SCOPE

2.1. The Policy shall be applicable to all companies of the Group and shall be binding on all Employees of the Group Companies and persons performing their job functions under other contractual arrangements, such as trainees or temporary employees, service providers and other third parties who use or are directly connected to the Group's information resources, regardless of their location.

2.2. Each Company shall familiarise its employees with the Policy and its supplementary documents in accordance with the procedures established by the Company.

2.3. Third parties shall ensure compliance with the requirements of this Policy on the basis of contracts signed or other legally binding commitments made in accordance with the provisions of this Policy and its implementing legal acts. Third parties, employees of which perform activities at the Company, shall ensure that such employees are familiarised with this Policy and are informed of their obligation to comply with it.

2.4. The Policy and other relevant documents shall be reviewed at least once a year and, if necessary, amendments shall be initiated.

2.5. The Policy shall be publicly available on the Group's internal website and on its website.

3. GENERAL PROVISIONS

3.1. This Policy has been prepared on the basis of EU and national legislation, and describes their application and implementation in the Group’s activities related to information security and personal data protection.

3.2. The main legal acts governing information security in the Group are the following:

3.2.1. The Law on Cybersecurity of the Republic of Lithuania, which transposes the requirements of the EU's TIS2 (Directive on Security of Network and Information Systems) into Lithuanian law;

3.2.2. General Data Protection Regulation (**GDPR**);

3.2.3. The Law on Legal Protection of Personal Data of the Republic of Lithuania No. XIII-1426 of 30 June 2018 (hereinafter referred to as **LLPPD**).

3.3. The Policy has been prepared on the basis of the following documents, standards, as well as good practices in information technology (hereinafter referred to as IT):

3.3.1. Guidelines on Security Measures and Risk Assessment for Data Controllers and Processors (SDPI Guidelines);

3.3.2. LST EN ISO 27001:2022 "Information technologies – Security techniques – Information security management systems – Requirements" (hereinafter referred to as the ISO 27001 standard);

3.3.3. LST EN ISO 27002:2022 "Information technologies – Security techniques – Practice regulations for information security control measures" (hereinafter referred to as the ISO 27002 standard);

4. DEFINITIONS

4.1. **Personal Data** means any information about the person (data subject), such as name, surname, personal identification number, code provided in the system, image, passport copy, shoe or workwear size, IP address, browsing history, tablet geo-location data, etc. of the employee, customer) that would allow direct or indirect identification of a natural person.

4.2. **Company** means any company (regardless of its legal form) belonging to the Group, including the Management Company.

4.3. **Employee** means any employee of the Group working under an employment contract or on other contractual basis (e.g. apprenticeship contract, performance of contractual functions carried out on the basis of a self-employment agreement or a business licence) at a designated place of work and performing the functions assigned by the employer.

4.4. **Artificial Intelligence (AI)** means computer programs or algorithms capable of analysing data, making decisions, and performing tasks that would normally require human intelligence. They employ machine learning, neural networks, or other advanced methods to adapt, optimise, and operate in a dynamic environment.

4.5. **Information** encompasses all information and data, regardless of their form (soft copy, hard copy, or other) and storage location, related to the Company and/or the Group's activities, including but not limited to documents, photographs/video material, draft documents, copies, letters, memoranda, diagrams, plans, correspondence, contact details of the Group's clients and suppliers, software code, passwords, or any other information important to the Company's operations.

4.6. **Information Resources** means Group Information, managed Information Systems, services required for the functioning of information technology, knowledge of employees.

4.7. **Information Security** means the preservation of the confidentiality, integrity and availability of Information.

4.8. **Information System** includes software and information systems on the Group's servers, devices used by employees (computers, phones, tablets, external storage devices, network infrastructure, system (operating systems, archiving software, etc.), data, and any other computer components or systems owned by the Group or used for the purposes of the Group. Such information systems include all internal and external services, such as cloud computing services, internet access, email and communication tools.

4.9. **Hardware** encompasses any and all hardware owned by the Group, including but not limited to computers (including PCs, laptops, and tablets), external devices (USB disks or memory sticks, scanners, monitors, keyboards, mice, speakers, headphones, microphones, etc.), peripheral equipment (printers, copiers, scanners, fax machines, etc.), computer network equipment, projectors, cameras, uninterruptible power supplies, landline telephones, and similar devices.

4.10. **Visitor** means a customer, supplier's representative, service specialist, employee's guest and any person who comes to the Company's premises and is not an employee of the Company.

4.11. **Information Security Incident** means an event that compromises the integrity, confidentiality or availability of the Group's information and/or any of its information systems and violates or threatens to violate the law, this Policy, the Group's security procedures and the procedures governing the activities of Group companies.

4.12. **Confidentiality** means the preservation of permissible restrictions on access and disclosure, which is applied to ensure the privacy of personal data and the protection of trade secrets.

4.13. **Availability** means the property of information and information systems to be accessible when and where required.

4.14. **Integrity** means the property of information that ensures it remains throughout its lifecycle and has not been altered or destroyed accidentally or unlawfully.

4.15. **Cybersecurity Officer** means an employee appointed by the Group Chief Executive Officer to manage information security matters within the Group.

4.16. **Data Protection Officer (DPO)** means a person appointed by the Group's Chief Executive Officer to advise the Group on the requirements for the protection of personal data within the Group.

4.17. **User** means an Employee, supplier or other third party who is legally granted access to the Group's Information Resources.

4.18. **Group** means a group of companies comprising the Management Company and all the companies it directly or indirectly controls (including companies that are not part of the Group but have shares in that company).

4.19. **Management Company** means UAB Vičiūnų grupė, which for the purposes of this Policy is also referred to as the Company.

4.20. **VPN** means Virtual Private Network, a technological tool designed for secure access to the Company’s Information Resources.

5. RESPONSIBILITIES

5.1. The persons responsible for the management, supervision, and implementation of this Policy are:

5.1.1. the Board of the Group;
5.1.2. the Cybersecurity Officer;
5.1.3. the Data Protection Officer (DPO);
5.1.4. the Head of Infrastructure Unit;
5.1.5. all employees.

5.2. In the field of information security, **the Group's Board** shall be responsible for:

5.2.1. approving this Policy and establishing the objectives and principles for ensuring Information security within the Group;
5.2.2. granting authority and appointing responsible persons for Information and personal data security;
5.2.3. approving documents regulating information security;
5.2.4. determining the acceptable level of information security in the Group;
5.2.5. providing the necessary resources and facilities for the implementation of this Policy.

5.3. **The Cybersecurity Officer** shall be responsible for:

5.3.1. implementing and monitoring the implementation of the Policy (carrying out the control function);
5.3.2. examining and considering issues related to the security of Information Resources and use thereof;
5.3.3. examining, analysing and controlling issues related to Information Security events and incidents, cooperating with competent authorities;
5.3.4. organising annual and extraordinary (as required) Information security risk assessments;
5.3.5. ensuring that the Group complies with legislation regulating information security;
5.3.6. organising business continuity management plan tests;
5.3.7. submitting proposals and organising employee training on information security matters;
5.3.8. providing the System Administrator with recommendations related to the implementation of the Policy after pre-agreeing them with the IT Development Manager or a person designated by him;
5.3.9. cooperating with DPO on personal data protection issues.

5.4. **The Data Protection Officer** (hereinafter referred to as DPO) shall be responsible for overseeing the implementation of personal data protection requirements, and for carrying out the functions detailed in the Personal Data Policy.

5.5. **The Head of Infrastructure Unit:**

5.5.1. shall grant, modify, and revoke Users' access rights to the Group's Information Systems in accordance with clearly established company rules, and shall train and advise Users;
5.5.2. shall coordinate the operation of computer workstations and identify vulnerable areas;
5.5.3. shall ensure proper operation of computer network;

5.5.4. shall ensure the proper functioning of servers;
5.5.5. shall ensure the operation of databases and database archive, backup equipment;
5.5.6. shall be responsible for making backup copies of data, storing and restoring data from backup copies and security;
5.5.7. shall carry out the instructions and tasks of the Information Security Officer related to ensuring security (performs the function of implementing the measures).

5.6. **All Employees working with information systems and information** must:
5.6.1. comply with the information security requirements set forth in this Policy;
5.6.2. comply with the Personal Data protection requirements;
5.6.3. comply with confidentiality obligations, which shall be valid for the entire period of employment in the Group and after the termination or expiration of the employment or contractual relationship;
5.6.4. immediately report vulnerabilities, potential or actual information security events and incidents in accordance with the established information security incident management procedure;
5.6.5. use the Information Resources in accordance with internal procedures;
5.6.6. protect their password or other login or authentication data and not disclose it or share authentication tools (e.g. an unlocked smartphone) with others;
5.6.7. to comply with the requirements established for passwords and other authentication methods, such as PIN codes.

5.7. Consequences of non-compliance with the Policy:
5.7.1. Employees who fail to comply with or breach this Policy and related documents may be subject to disciplinary action for violation of work duties; in certain cases, the Company may also refer the matter to law enforcement authorities.
5.7.2. Possible consequences for Third Parties (or their employees) which/who fail to comply with or breach this Policy include termination of contracts, recovery of incurred losses, and other consequences stipulated for non-compliance with contractual obligations.
5.7.3. Ignorance, good intentions and/or incorrect decisions made shall not be considered as a justifiable reason for not compliance with this Policy.

6. COMPETENCIES

6.1. The persons responsible for the supervision and organisation of the implementation of the Policy shall possess thorough knowledge of information security, personal data protection and cybersecurity principles, and shall be guided in their activities by the laws and legal acts of the Republic of Lithuania regulating information security, cybersecurity and personal data protection. They must have knowledge of risk assessment methodologies and principles.

7. INFORMATION SECURITY RISK ASSESSMENT

7.1. The security of the Group's information is ensured through the implementation of risk-based security measures. The assessment of information security risks is an integral and inseparable part of the Companies' risk management process.

7.2. The Cybersecurity Officer shall be responsible for initiating, supervising, and continuously improving the information security risk management process, summarising collected information, communicating it, preparing the risk management plan, and control of its implementation.

7.3. The responsibility for the assessment of operational impacts and threats rests with the Company's Information Resource managers (owners), IT staff, and Employees according to their areas of competence.

8. INFORMATION SECURITY MEASURES AND OBLIGATIONS

8.1. Based on risk management, the Group has established the organisational and technical information security measures to ensure the security of information that include, but are not limited to:

8.2. **Responsibility for assets:**

8.2.1. Information and the Hardware used for its processing shall have a designated materially responsible person. This person shall be responsible for the confidentiality, integrity and availability of such Hardware and Information.

8.2.2. Information and Hardware shall be assigned on the conclusion of an employment or other contract and shall be returned at the end of the employment or other contract.

8.2.3. The Group has established a **Register of Information Resources**, in which Information Systems and technical means used for processing information, including Personal Data (computer workstations, servers, network equipment, information systems), are identified, and Information Resource owners responsible for the proper maintenance of the assigned Information Resources and for establishing the information security requirements applicable to it are assigned. The register shall be reviewed and updated on a regular basis, every 3 months, under the responsibility of the Cybersecurity Officer.

8.2.4. All Group Information Resources shall be accounted for and documented, identifying the manager of the resource (or a group thereof), the related technical information, and the physical location.

8.3. **Security in the use of Information Resources:**

8.3.1. All Information Resources may only be used for the Group's operational functions.

8.3.2. Each Employee must be formally informed in writing of the requirements applicable to his/her use of Information Resources.

8.3.3. Before termination of employment, all assigned Information Resources (means for storing, transmitting, and processing information, documentation, portable data carriers) must be returned to the Company.

8.4. **Clean desk and clean screen policy:**

8.4.1. Staff must follow a "clean desk and clean screen" policy, i.e. turn on a password-protected screen saver when leaving the workstation, turn off all applications and the computer at the end of the workday, place documents and data media on the desk in drawers or cabinets, or, in the case of information that is confidential or constitutes a

commercial/manufacturing secret, in lockable drawers and cabinets, or in safes, and permanently destroy documents and data media that are no longer needed, either sensitive or confidential.

8.5. **Teleworking security:**

8.5.1. The Company must ensure secure teleworking and use of mobile devices.

8.5.2. For remote access, only secure access methods and tools provided by the Company may be used. Employees of the Company shall only be permitted to access the Company's Information Resources from computers provided by the Company for their work. Unauthorised remote access to the Company's Information Resources shall be strictly prohibited.

8.5.3. Remote access to the Company's Information Resources (e.g. access to cloud services, VPN access to internal computer network resources, etc.) via public networks (the Internet) shall be implemented using mandatory two (or more) factor authentication; therefore, in order to additionally authenticate the identity of the connecting party, a mobile phone linked to the Company's Information Resources shall be used.

8.5.4. The Company shall have the right to manage mobile devices and the software installed on them using software tools.

8.5.5. Remote Users shall be responsible for preventing third parties from accessing the Company's Information Resources during the login session, i.e. when leaving their workstation, they must disconnect from the internal network and lock their computer.

8.5.6. An Employee must comply with this Policy and other applicable laws and regulations of the Company, regardless of whether he/she is working on the Company's premises or remotely.

8.6. **Classification of information:**

8.6.1. Company information shall be classified according to security needs and legal requirements. The list of confidential information and information constituting trade (production) secrets, as well as the requirements for information management, are set out in the **Confidentiality Agreement** of Vičiūnai Group.

8.7. **Management of access rights:**

8.7.1. When managing access to the Company’s information resources, the principles of "need-to-know" and “least privilege access” must be ensured, i.e., access to the Company’s information resources may only be granted to authorised individuals and only to the extent necessary to perform specific work duties and other functions related to the Company.

8.7.2. Access management must be documented. Access rights of users and administrators to information systems shall be reviewed at least once a year as well as in the event of significant changes in the Company or security incidents.

8.8. **Use of cryptographic measures:**

8.8.1. In order to ensure the secure transmission/receipt of electronic information, data shall be transmitted over encrypted data channels using specific protocols.

8.9. **Backup creation and management:**

8.9.1. Backups of all data and software critical to the Company's operations must be performed periodically. Restoration from backups must be tested at least once a year, with the test results reported to the Cybersecurity Officer. Backups must be stored at a safe distance from the primary systems – in a secondary data centre, cloud service systems. The frequency, volume, methods and retention period of backups shall meet the system's RTO (Recovery Time Objective) and RPO (Recovery Point Objective) requirements.

8.10. **Management of vulnerabilities:**

8.10.1. All workstations, servers, network devices, etc. must have security patches installed to protect Information Systems from vulnerabilities.

8.11. **Security of information transmission:**

8.11.1. The Group uses data security technologies. When transmitting confidential information or information intended for internal use through any channel (e-mail, SFTP, HTTPS, etc.), strong encryption algorithms must be used.

8.11.2. When transferring paper documents, the data must be inventoried and properly recorded before the transfer.

8.11.3. Before placing information on a chosen external storage medium, users must comply with the information classification requirements.

8.12. **Management of changes:**

8.12.1. The purpose of change management is to synchronise and control all changes made to the Information Systems in which Group Information and Personal Data are processed. This is an important security measure, as failure to implement the changes could lead to unauthorised disclosure, modification or destruction of data.

8.12.2. The need for changes may arise for a variety of reasons, including but not limited to the following:

- approved user requests;
- changes to supplier services;
- hardware or software updates;
- new hardware or software installations;
- infrastructure changes.

8.12.3. The Company shall ensure that all changes to the Information Systems are monitored and recorded by a designated person (System Administrator).

8.13. The Group uses measures to protect against malicious software code.

8.14. **Event logging and monitoring:**

8.14.1. The Group shall have the right and obligation to monitor all Information Systems, including all devices that connect to or use the Information Systems, and to monitor (log) all data stored on the Group's Information Systems and/or transmitted over the Group's networks. An example of such logging is the collection of log entries, e.g., recording an employee's login to a specific information system. Such monitoring does not imply

monitoring or controlling the actions of Employees for the purpose of assessing the quality of performance of their job duties.

8.15. The Group uses Network Management Tools.

8.16. **Data retention, deletion, disposal:**

8.16.1. data that is no longer needed must be securely destroyed. Electronic data shall be irretrievably deleted or the media shall be destroyed, paper data shall be destroyed with a document shredder.

8.16.2. When data media are removed (end of life) or temporarily transferred (e.g. for repair) from the working environment, the data must be encrypted with appropriate security encryption algorithms or destroyed.

8.16.3. The Group avoids the use of external storage media, such as data carriers, CDs/DVDs, etc., except in extreme cases.

8.16.4. Destruction of computer media and the information contained therein shall be carried out by the employees responsible for Hardware maintenance.

8.17. **Security in the use of artificial intelligence systems:**

8.17.1. Given the frequent use of AI systems in today's working environment, it is also necessary to consider the risks posed by such systems.

8.17.2. Improper use of AI systems may result in the disclosure of the Company's confidential information or other intellectual property when used improperly (e.g., public or private AI services are used for work-related tasks), when the Company's information is made available to such systems, and is then used to train the systems and in other ways without the Employee's knowledge or control.

8.17.3. Any use of AI systems to process the Company's information or confidential information of business partners or third parties without assessing their risks shall be prohibited. The assessment of potential risks must involve specialists with sufficient knowledge in the field of AI.

8.17.4. The Company may provide Employees with access to isolated AI systems (which do not exchange information with public networks, i.e., the Internet) that are authorised by management for use within the Company.

8.17.5. The results obtained using AI systems must be critically evaluated and further verified, taking into account that AI systems may provide false information.

9. PHYSICAL AND ENVIRONMENTAL SAFETY

9.1. The security of information resources within the Company must be ensured as part of the Company’s physical security system.

10. RELATIONS WITH SUPPLIERS AND OTHER THIRD PARTIES

10.1. Access to the Group's Information and/or Information Resources may be granted to Suppliers only to the extent necessary for the implementation of the contract and shall be immediately terminated upon termination of the contractual relationship.

10.2. Contracts with suppliers which are to be granted access to the Group's Information and/or Information Resources must include the Minimum Information and Cybersecurity Requirements for Suppliers (Annex No. 1).

11. SECURITY of HUMAN RESOURCES

11.1. Before being granted access to the Company's Information Resources, a person must be formally informed in writing of his/her information security obligations and responsibility as set out in the employment contract, the Personal Data Processing Policy, the Information Security Policy, the Rules of Procedure, and other internal documents.

11.2. Contracts with Third Parties must include the information security obligations and responsibilities of the parties.

11.3. The Company's Employees and, where applicable, Third Parties must have sufficient knowledge of information technology, telecommunications, and information security to perform their job functions. Each Employee must be trained to recognise information security threats/incidents, to apply security measures and techniques, and to report information security incidents.

11.4. The level of safety knowledge of employees must be assessed and, if necessary, additional training must be provided.

12. MANAGEMENT OF INFORMATION SECURITY INCIDENTS

12.1. All information security incidents and events (such as loss of equipment or information, computer viruses, breaches of this Code of Conduct, etc.) or security gaps or weaknesses must be immediately reported to the **Cybersecurity Officer** and the IT Department by **e-mail: soc@vici.eu, it-help@vici.eu** or by phone +370 67059912.

12.2. All Employees, Third Parties, and other relevant persons are obliged to report security incidents, clearly specifying the reporting methods and the individuals responsible for making such reports.

12.3. Information security incidents (and security events) shall be managed in a systematic and consistent manner, ensuring an appropriate and timely response and mitigation of the future impacts, as set out in the Information Security Incident Management Process.

12.4. Information on security incidents, "lessons learnt" and suggestions for improving incident management shall be monitored using indicators and discussed during meetings. This information shall also be used for risk identification and monitoring.

12.5. The management of Personal Data breaches shall be governed by the Company's Personal Data Breach Response Procedure. The Data Protection Officer shall be involved in the management of Personal Data security incidents.

13. BUSINESS CONTINUITY MANAGEMENT

13.1. Business continuity management in case of information security incidents shall be integrated into the Company's business continuity system and managed with uniform requirements across the organisation.

13.2. An information system continuity/recovery plan must be in place for each information system that is essential to the Company's operations.
13.3. The effectiveness of the business continuity plan shall be tested annually by simulating critical situations, during which designated responsible persons carry out the necessary actions. Identified deficiencies and vulnerabilities shall be analysed, and improvement measures shall be determined.

14. INFORMATION SECURITY AUDIT

14.1. The Company's information security audit and assessment of compliance with the requirements of the legal acts of the Republic of Lithuania shall be carried out periodically, but not less than once a year. The assessment shall be carried out by the Company's Cybersecurity Officer.
14.2. The assessment of the Company's compliance with the Personal Data protection requirements shall be carried out at least once a year. Such assessment shall be carried out by the Data Protection Officer.
14.3. The external Information Security Audit shall be carried out every 3 years. The audit shall be carried out by the Group's audit division or by firms with qualified professionals with at least 3 years of experience in information security auditing.
14.4. The recommendations and non-conformities identified during audits must be evaluated, and an action plan for improving information security must be developed.

ANNEXES

No. 1 Minimum Information and Cybersecurity Requirements for Suppliers