Normative internal legal act	**Information Security Policy of AB "Ignitis grupė" group of companies**
Name of the process	Information security management
Process owner (unit)	UAB "Ignitis grupės paslaugų centras" Digital Security
Approving company	AB "Ignitis grupė"
Approving person/body	Management Board of AB "Ignitis grupė"
Date of entry into force	01/10/2024

INFORMATION SECURITY POLICY OF AB "IGNITIS GRUPĖ" GROUP OF COMPANIES

1. PURPOSE AND SCOPE

1.1. The purpose of the Policy is to set out directions and principles for ensuring the Group's Information Security and the obligations of recipients and users of the Group's information in order to ensure the protection of the Group's information against unauthorised acquisition, use and disclosure; as well as to ensure the integrity and availability of the Group's information and to manage Information Security risks within the Group to an acceptable level.

1.2. The Policy covers all information of the Group, regardless of its form and nature, which is entered, transmitted or stored in the Group's Information Systems and/or Cloud service systems. The Policy also covers Employees' use of devices which are issued by the Group or connected to the Group's Information Systems and/or Cloud service systems, including but not limited to mobile phones, tablets, laptops and desktop computers.

1.3. The Policy shall apply to all Group Companies and shall be binding on all Employees of Group Companies and Service Providers.

1.4. Group Companies which are registered and operate in foreign countries shall apply this Policy to the extent that it does not conflict with the legislation of these countries.

2. TERMINOLOGY

2.1. The Glossary contains general terms: Acceptable Risk Level, Access Rights, Account, Cloud, Company, Confidential Information, Critical Process, Data, Employee, Group, Group Service Centre, Information, Information Assets, Information Asset Owners, Information Security, Internal Legal Act, IT, OT, Parent Company, Remote Workstation, Request Management System.

2.2. **Information System** means an IT or OT system.

2.3. **External Storage Device** means any type of data storage device (electronic, magnetic or optical) which is not part of the Device (e.g. USB sticks, external hard drives, CDs, DVDs, etc.).

2.4. **Device** means a telephone and/or computer (tablet, laptop, desktop computer, etc.) and/or their accessories.

2.5. **Collegial Body** means a collegial management body, i.e. the Management Board/Board, and/or a supervisory body, i.e. the Supervisory Board, as specified in the founding documents of the Parent Company and/or Companies.

2.6. **Mobile Device** means a laptop, tablet, mobile phone.

2.7. **Service Provider** means a Third Party that provides services to Companies.

2.8. **Policy** means the Information Security Policy of AB "Ignitis grupė" group of companies, this document.

2.9. **Third Party** means a natural person or a legal entity outside the Group.

3. GENERAL PROVISIONS

3.1. The Group's Information is a valuable part of the assets of Group Companies. Its loss, unauthorised acquisition, alteration or disclosure may have a negative impact on the achievement of the Group's and/or Companies' strategic objectives as well as competitiveness, image and reputation.

3.2. Group Companies operate in the economic sector which is important to the national security of the Republic of Lithuania and therefore it is of particular importance to ensure the confidentiality, fairness, integrity and availability of Information. In order to protect the Information and Information Systems of customers, partners, contractors and the Group, the Group places great emphasis on the security of Information and Information Systems as well as on the processes of recruitment and termination/end of employment, the development of Employees' competences during their employment within the Group as well as the assessment of the competences and reliability of Third Parties and/or their employees.

3.3. The provisions of this Policy shall be applied taking into account the requirements as set out in the legislation of the Republic of Lithuania or in the relevant legislation of a foreign country. If there are discrepancies between the legislation and the Policy, the Policy shall be applied to the extent that it does not conflict with the legislation. The Policy shall also be applied in accordance with international standards and/or best practice, including:
   3.3.1. International Standard ISO/IEC 27001 *Information security, cybersecurity and privacy protection – Information security management systems – Requirements*;
   3.3.2. Lithuanian Standard LST EN ISO/IEC 27002 *Information security, cybersecurity and privacy protection – Information security controls (ISO/IEC 27002:2022)*, which has been transposed from European Standard EN ISO/IEC 27002:2022 *Information security, cybersecurity and privacy protection – Information security controls;*
   3.3.3. International Standard ISO/IEC 27017 *Information technology - Security techniques - Code of practice for information security controls based on ISO/IEC 27002 for cloud services*;
   3.3.4. International Standard ISO/IEC 27018 *Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*;
   3.3.5. International Standard IEC 62443 *Industrial communication networks – Network and system security*.
3.4. The Group Service Centre, which provides Information Security services to Group Companies, must be certified in accordance with the international standard referred to in paragraph 3.3.1 of this Policy and must ensure that Third Parties engaged to provide services meet the requirements as set out in the legislation and the Policy and that they act in accordance with international standards and/or best practice.
3.5. In order to achieve the objectives of this Policy, the Group shall have a cyber incident response team “Ignitis CERT”, which shall act in accordance with international principles and standards for cyber incident response (“CERT/CSIRT”) teams, participate in organisations which bring together global CERT/CSIRT teams, including TF-CSIRT, and maintain the status of an accredited member of the TF-CSIRT organisation.
3.6. The provisions of the Policy shall be set out in detail in the Group’s and/or the Parent Company’s and/or a Company’s internal legal acts, which must not be in conflict with this Policy.
3.7. The Head of Digital Security at the Group Service Centre shall approve any exceptions to the application of the provisions of the Policy in the Request Management System or by electronic means, ensuring traceability.

4. DIRECTIONS AND PRINCIPLES FOR ENSURING INFORMATION SECURITY

4.1. **Training and education.** The Group shall develop a culture of Information Security to ensure that Employees properly understand the importance of Information and its security and the potential negative impact of unauthorised acquisition, alteration, use and disclosure of Information on the Group’s activities and on the achievement of the goals set for Companies. The aim is to continuously increase Employees’ resilience to Information Security threats by periodically organising training, testing Employees’ knowledge, regularly communicating about Information Security threats relevant to the Group and controls which prevent Information Security incidents. In addition, Employees delegated by Group Companies shall participate in cyber security exercises organised by the North Atlantic Treaty Organisation (NATO) and/or the Republic of Lithuania.
4.2. **Clear ownership.** Information Assets which are of the highest value, including the confidential information and commercial (industrial) secrets of Companies, must be identified, and responsible Information Asset Owners must be designated. The Group must also have designated owners of IT services and systems and OT devices who have a right to make decisions, manage necessary resources and are responsible for the proper management of Information Security.
4.3. **Risk management.** The Group’s Information Security management system shall be based on the identification, assessment and monitoring of risks. The risks of Information Security threats to the Group’s Critical Processes and Information Systems must be assessed periodically and as necessary (e.g. when new Information Systems and business processes are developed or existing ones are modified). Identified risks must be mitigated to an Acceptable Risk Level through the application of Information Security controls which are risk-based, cost-effective and in line with international standards for Information Security. Threats of physical and natural origin must also be assessed in the Information Security risk assessment.

4.4. **Compliance.** The Group shall implement the requirements for Information Security as set out in the legislation, taking into account the regulatory framework in the country in which a Company operates, and shall implement contractual and other obligations of Companies through the application of risk-based Information Security controls.
4.5. **Relations with Third Parties.** The security of Information which is provided and/or received in the course of pre-contractual and/or contractual relationships with Third Parties must be ensured throughout the duration of pre-contractual and/or contractual relationships and/or obligations, or beyond, including, but not limited to, the inclusion of Information Security provisions in agreements and contracts, obliging the recipients of Information to ensure a level of Information Security which is not lower than that applied within the Group. The Group shall cooperate with the institutions of the Republic of Lithuania which develop and implement cyber security policy, shall participate in professional forums and share information related to Information Security and its threats as well as best Information Security practice with other companies and organisations.
4.6. **Threat intelligence, management of incidents and vulnerabilities.** The Group shall carry out continuous threat intelligence by collecting and analysing information which is related to Information Security threats. Information security incidents, events and vulnerabilities shall be systematically and consistently identified, assessed and managed, ensuring appropriate response, containment and the provision of controls to prevent the recurrence of incidents or the exploitation of vulnerabilities.
4.7. **Information Security in the management of projects and changes.** Information Security must be integrated into all phases of change projects. Before initiating new projects regarding Information Systems and Cloud service systems or planning major changes, potential Information Security risks must be assessed and appropriate Information Security controls must be selected.

5. PARTICIPANTS INVOLVED IN ENSURING INFORMATION SECURITY AND THEIR OBLIGATIONS

5.1. All participants who are involved in ensuring the Group's Information Security (those involved in Information Security management processes) shall have an obligation to comply with this Policy, Information Security requirements as laid down in the legislation and pre-contractual and/or contractual obligations.
5.2. The **Management Board of the Parent Company** shall approve this Policy and shall set out directions, objectives, aims and principles for ensuring Information Security within the Group.
5.3. **Employees** shall ensure Information Security in their day-to-day activities in the performance of their job functions and in decision-making by identifying, assessing and monitoring Information Security risks and selecting controls to manage them as well as aligning these decisions with Information Security requirements. Employees shall be responsible for compliance with Information Security requirements and for the secure use of Information Assets which are entrusted or known to them.
5.4. **CEOs of Companies** shall ensure that Information Security requirements are integrated into activity planning processes and shall consider Information Security risks as an integral part of Companies' activity processes as well as pay due attention and allocate adequate resources to ensure Information Security and manage identified risks.
5.5. The **Digital Security Unit** at the **Group Service Centre** shall develop the Group's Information Security Strategy, organise the identification and assessment of the Group's Information Security risks and their management to an Acceptable Risk Level, provide assistance to Companies in the management of risks and monitor the need for, and the appropriateness and implementation of, the Group's internal legal acts regulating Information Security.
5.6. **Service Providers** shall ensure that their infrastructure and processes meet Information Security requirements which are imposed on them and shall be responsible for compliance with Information Security requirements and for the secure use of the Group's Information Assets.
5.7. **Other Interested Parties** are persons with interests or rights related to Information Security, including the Republic of Lithuania, shareholders of the Parent Company and/or Companies, customers of Group Companies, residents of the countries in which Group Companies operate, persons providing goods and services to Group Companies, and other Third Parties.

6. MANAGEMENT OF INFORMATION ASSETS

6.1. All non-public Information is the property of the Group and must be protected by Employees and Service Providers.

6.2. All Group Information shall be classified into classes based on its importance and the extent of the potential damage caused by its disclosure or loss and shall have the following markings:
  6.2.1. information for public use (without a marking);
  6.2.2. information for internal use (marked INTERNAL USE);
  6.2.3. confidential information:
    6.2.3.1. for external reciepents (marked CONFIDENTIAL);
    6.2.3.2. for internal reciepents (marked CONFIDENTIAL);
  6.2.4. strictly confidential information, intended for specific recipients only (marked STRICTLY CONFIDENTIAL).
6.3. Information for public use is of the lowest class and Strictly Confidential information is of the highest (most protected) class.
6.4. Each Group Company must approve a list of Confidential Information and Commercial/Industrial Secrets, which is drawn up in accordance with the model list of Confidential Information and Commercial/Industrial Secrets as approved by the Management Board of the Company. Information contained in these lists shall be classified as Strictly Confidential or Confidential Information.
6.5. The use, transfer and management of Information shall be subject to security controls as set out in the Standard for Ensuring Confidentiality of the Group Information.
6.6. The Group's personal data protection controls and responsibilities are set out in the Group Personal Data Protection Policy and related legal acts.

7. INFORMATION SECURITY CONTROLS AND OBLIGATIONS

7.1. The Group shall implement organisational and technical Information Security controls which are based on innovative security solutions and are proportionate to the identified risks. Detective, preventive and corrective risk management controls shall be applied following an assessment of potential risk factors to the Group's Information.
7.2. The Group's Information Security management system shall include (but shall not be limited to) the following organisational and technical controls:
  7.2.1. **Management of Access Rights:**
    i. Access Rights to Information Assets within the Group shall be granted by a decision of the Information Asset Owner on a need-to-know basis;
    ii. Accounts for Information Systems and Cloud service systems, operating systems and databases managed by the Group, including access to software code, must be centrally managed through the Request Management System;
    iii. Information Asset Owners must review Access Rights granted to Information Assets at least once a year, ensuring that these Access Rights are granted on a need-to-know basis and that unnecessary Access Rights are removed immediately;
    iv. Secure authentication controls shall be used for access to Information Systems and Cloud service systems;
    v. Where Access to Information Assets is granted to Third Parties, confirmation must be obtained from Third Parties that Access will be used in accordance with this Policy and other Information Security requirements, only for the purpose, to the extent and in the manner specified, and liability for the violation of this obligation must be provided for.
  7.2.2. **Security of data networks:**
    i. The perimeter security of data networks shall be ensured through the use of firewalls and continuous monitoring between the Group's internal network and the public communications network (the Internet);
    ii. The Group must ensure that the OT data network is physically separated from the IT data network;
    iii. The Group's Data Network shall be segmented into separate network security zones based on the importance of Information Systems and the identified risks;
    iv. The Group's Information Assets can only be accessed from a Remote Workstation using an encrypted connection;
    v. The security of data transmission shall be ensured in accordance with the Group's Standard for Ensuring Security of IT/OT systems as approved by the Head of Group IT.
  7.2.3. **Operational security of Information Systems:**
    i. The Group's Information Systems must have controls to detect, prevent and monitor malicious software and/or activities;

ii. Security logs of all Information Systems, Data Network devices and Devices, including operating systems, databases and applications, must be centrally stored within the Group.

7.2.4. **Security of Devices:**

i. Devices must meet security requirements as set out in the Group's internal legal acts. The settings of all Group Devices shall be managed by the Group's IT function;

ii. Devices, e-mail and Internet resources provided to Employees are for the performance of their job functions, and the internal legal acts of the Group and/or a Company shall determine the conditions of their use for personal purposes;

iii. It shall be assumed that Mobile Devices are frequently used in insecure environments and face a higher digital security risk, therefore, they shall be subject to at least as effective security controls as those which are used in Devices in the regular workplace;

iv. The use of personal Devices, other than mobile phones, is prohibited on the Group's network. Personal mobile phones may be used in accordance with the procedure set out in the Group's internal legal acts;

v. The Group's Information and work applications on mobile phones and tablets shall only be accessed using a Mobile Device Management (MDM) solution;

vi. Cloud service systems which are managed by the Group shall only be accessed from Group-managed Devices. An exception may be made for members of the Collegial Bodies of the Parent Company and Companies.

7.2.5. **Human factor:**

i. Employees, members of Collegial Bodies, Service Providers and/or other Third Parties shall have an obligation to protect the Group's Information Assets. The Group shall ensure that written commitments to protect Confidential Information are included in employment contracts and contracts with Service Providers and that these commitments are obtained prior to the commencement of a contractual relationship or when Information Assets are provided to Third Parties on any basis;

ii. Prior to any recruitment or transactions with Third Parties, the screening of selected candidates and Third Parties must be carried out in accordance with the Group's internal legal acts;

iii. Employees and/or members of Collegial Bodies shall be granted such Access Rights to Information Assets as are necessary to perform their functions and only after they have become acquainted with the Group's internal legal acts regulating Information Security;

iv. Employees shall get acquainted with the Group's legal acts regulating Information Security on a periodic basis. The Group must organise Information Security Awareness training to at least once a year and must test Employees' knowledge and skills to resist Information Security threats;

v. Access Rights to Information Assets must be removed immediately upon termination of an employment and/or civil legal relationship.

7.2.6. **Cryptography:**

i. The security of the Group's Information Assets must be ensured through the use of generally accepted secure encryption tools, the requirements for which shall be set out in the Group's internal legal acts;

ii. Cryptographic keys must be centrally managed using a key management system;

iii. Encryption tools must be used on all Mobile Devices, External Storage Devices and Data Networks in accordance with the Group's internal legal acts;

iv. In order to identify malicious code, encrypted traffic on Data Networks can be decrypted for analysis purposes.

7.2.7. **Physical protection:**

i. Physical access to the Group's offices and other premises where the Group's Information Assets are stored shall be restricted and controlled by means of preventive and detective controls;

ii. Physical protection controls (e.g. clean desk and computer screen) shall be applied both in offices of Companies and Remote Workstations.

iii. Any other internal legal acts of the Group and/or a Company which regulate the Group's physical protection must also be followed to ensure the physical protection of the Group.

7.2.8. **Management of vulnerabilities:**

i. The Group must periodically identify, assess, monitor and remove vulnerabilities in the IT and OT components of Information Assets;

ii. Identified vulnerabilities must be classified and removed in order of priority, based on their level of criticality.

7.2.9. **Acquisition, development and maintenance of Information Systems:**

i. Information Systems which are newly designed, developed and acquired and changes to existing ones must meet security requirements as set out in the legislation;

ii. A security assessment must be carried out prior to the use of Information Systems or parts thereof. The use of Information Systems which do not meet security requirements is prohibited;

iii. Information Systems and their components (operating systems, database management systems, other related software) which are used within the Group must be supported by the manufacturer and periodically updated;

iv. The life cycle of Information Systems which are used within the Group must be assessed and planned;

v. Information Systems or components thereof which are no longer used must be turned off or archived. When a decision not to use an Information System is made, the means of storing or destroying Information Assets must be provided, taking into account the requirements as set out in the legislation.

7.2.10. **Relations with Third Parties:**

i. Third Parties that provide IT/OT services and/or Cloud services to Group Companies or manage the Group's Information Assets must ensure that their infrastructure and processes meet security requirements which are imposed on them;

ii. Third Parties must sign a confidentiality commitment, get acquainted with this Policy and comply with it;

iii. Service Providers shall be granted access to the Group's Information Assets necessary for the provision of services through the Request Management System;

iv. Monitoring and registration of the actions of Third Parties that provide IT/OT services must be ensured;

v. Agreements for the provision of Cloud services must include provisions on service availability, data confidentiality, security controls applied by a Service Provider, compliance with standards and legislation, management of incidents and vulnerabilities, liability and compensation for losses, suspension and termination of services, ensuring the transfer or destruction of Group data.

7.2.11. **Management of incidents:**

i. Employees, members of Collegial Bodies, Service Providers and other Third Parties shall have an obligation to report Information Security incidents they observe;

ii. The management of information security incidents must include the identification, assessment, categorisation and prioritisation of an incident, taking into account the impact, containment and elimination of the incident;

iii. Lessons learned from the management of incidents must be applied to prevent incidents and/or reduce the likelihood and impact of future incidents;

iv. Relevant state institutions, citizens and/or Service Providers must be informed about Information Security incidents which occur and/or have occurred within the Group in accordance with the procedure set out in the legislation.

7.2.12. **Risk management and business continuity:**

i. Periodic identification, assessment and monitoring of Information Security risks shall be carried out in accordance with the Group's Risk Management Policy;

ii. Business continuity shall be ensured in accordance with the Group's Policy for Ensuring Business Continuity.

7.2.13. **Compliance and audit:**

i. Information Security obligations of Group Companies to Third Parties and Information Security requirements which are set out in the internal legal acts of Group Companies and in the external legislation (depending on the country in which a Group Company operates) must be implemented through risk-based Information Security controls;

ii. Information Security audit must be carried out on a periodic basis, at least once every 2 years, or in the event of major organisational, systemic or other changes. Measures for auditing Information Security cannot stop Companies from operating.

8. LIABILITY

8.1. If an Employee violates the provisions of this Policy, such a violation may be considered a serious breach of work duties, which may be subject to the consequences set out in the Labour Code of the Republic of Lithuania, including but not limited to the termination of the employment contract at the initiative of the employer, due to the fault of the Employee.
8.2. Pre-contractual relations and contracts of Group Companies, including employment contracts, must ensure compliance with the confidentiality obligation by setting out in writing the obligation of the parties to keep secret any information communicated to each other or otherwise made known to each other both throughout the duration of the pre-contractual or contractual relationship and beyond and by agreeing on penalties and compensation for losses in the event of any violation of the confidentiality obligation.
8.3. When entering into transactions with Third Parties, the obligations of a Third Party to comply with the provisions of this Policy must be included as well as specific Information Security requirements which are in line with this Policy and which are required by the nature of a transaction, and liability for non-compliance with the provisions of this Policy, including the right of a Group Company to terminate the transaction unilaterally and to claim penalties and compensation for losses, must be provided for.

9. FINAL PROVISIONS

9.1. All current and newly employed Employees, members of Collegial Bodies, Service Providers and other Third Parties who perform contractual obligations must get acquainted with the Policy and undertake to meet its requirements. Employees must get acquainted with the Policy by means which provide evidence of acquaintance.
9.2. This Policy must be applied not only in accordance with the legal acts which are set out in this Policy but also with the Group's other legal acts relating to and/or detailing and/or supplementing this Policy.
9.3. The Policy must be reviewed at least once a year and updated as necessary.
9.4. This Policy shall be published in the Group's centralised document management system.

10. RELATED LEGAL ACTS

10.1. *Group Risk Management Policy*;
10.2. *Group Policy for Ensuring Business Continuity*;
10.3. *Group Personal Data Protection Policy*;
10.4. Standard for Ensuring Confidentiality of the Group Information.
10.5.