

## INFORMATION SECURITY POLICY

**PRIORITY** We consider information to be a priority resource for our activities, therefore the security of electronic, written and verbal information is a fundamental goal in order to ensure the reliability, financial stability, continuity of operations and the fulfillment of the requirements of interested parties of the closed joint-stock insurance broker company "IVP Partners" (hereinafter – “the Company” or “we”).

---

**OBJECTIVE** The Information Security Policy (hereinafter - the Policy) defines our position and responsibility of the Company's management in the field of information and cyber security. It is intended to present unified principles of security management and ensure effective implementation of the Company's information security management process.

The following high-level objectives have been established:

- > 100 % completion of information security training;
  - > Achievement of the defined Business Continuity RTO and RPO targets;
  - > Annual maintenance of the ISO 27001 certification.
- 

**SCOPE** This Policy is binding on all employees, shareholders and management of the Company, including freelancers - service providers.

The policy applies to every location, activity and process of the Company, where information is stored, transferred or otherwise processed, regardless of its form and storage method.

---

**MANAGEMENT SYSTEM** The Company carries out information security management based on the requirements of the international standard ISO/IEC 27001:2023, the implementation of which is annually audited and certified by an external auditor - the public certification institution "LST Sert" (legal entity code – 300076307, registered in Lithuania).

---

**SECURITY DIRECTIONS**

- > The Company’s management ensures that the necessary resources are provided for the implementation and maintenance of the Information Security Management System (ISMS).
- > The Company’s management ensures that ISMS objectives are aligned with the organization’s strategic direction.
- > Information security roles and responsibilities are assigned and communicated.

**PRINCIPLES** **Attention to the development and maintenance of information and cyber security culture.** Employees are educated to properly understand the importance of information and its security, the possible negative impact on the Company's activities and the implementation of strategic goals. The resilience and awareness of cyber threats of all the Company's employees is constantly being increased by periodically organizing trainings, carrying out continuous communication about current threats and measures to avoid incidents.

**Risk assessment and management.** The relationships of the company's most important operational processes and information storage sources with various possible threats are evaluated periodically. Identified risks are reduced to a tolerable risk level by applying security measures based on risk assessment, balanced in terms of cost and effectiveness.

**Compliance.** Ensure compliance with information and cyber security requirements established in legal acts, the Company's contractual obligations with third parties: partners, insurers and customers.

**Systematic management of incidents and vulnerabilities.** Managing information security and cyber incidents ensures the necessary response, containment and prevention of future incidents.

**Testing.** Annual internal and external system testing is carried out, ensuring the lowest possible vulnerability.

**Asset and information classification.** The Company's internal documents define the classification of documents and the assignment of information asset owners.

**Access management.** The principle of least privilege is applied, supported by a role-based access control system and multi-factor authentication for critical resources.

---

**RESPONSIBILITY** Any violation of Information Security norms is considered to be an Information Security Incident, which may have a negative impact on the continuity of the Company's activities, damage and harm the Company's image in society and the business environment.

Immediately notify the Company's management by e-mail upon noticing a malfunction of the Company's information systems or a security incident, a cyber security gap or a weak spot by mail [info@ivp.lt](mailto:info@ivp.lt) or by phone +370 5 219 7601.

The measures provided for in the laws of the Republic of Lithuania, internal legal acts of the Company and contracts, agreements or other legally binding documents are

applied to the Company's employees and third parties who have violated the requirements of the information security management system.

---

**OBLIGATIONS** The Company commits to complying with all information and cybersecurity obligations established in the legislation of the European Union and the Republic of Lithuania, as well as in contractual agreements, and to regularly evaluate the Information Security Management System, conduct internal audits and risk assessments, implement corrective actions, and ensure the continual improvement of the system.

---

**POLICY REVIEW AND DISTRIBUTION** The policy is approved, changed or deleted by the decision of the Company's management. The policy is prepared, regularly reviewed and updated by the Company's information security specialist.

The policy is published publicly on the Company's website [www.ivp.lt](http://www.ivp.lt) and is available to all interested parties.

The provisions of this Policy are detailed and implemented by adopting the Company's internal documentation, which is compatible with the Company's strategic goals, legal requirements, international information security standard, third party requirements and good practices.

---

Approved: 17 11 2025, version No. 4